

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

EXAMINATION INDEX

EXAMINATION OF		PAGE
DANIEL ALFIN	DIRECT EXAMINATION	54
	By Mr. Becker	
	CROSS-EXAMINATION	73
	By Mr. Fieman	
	REDIRECT EXAMINATION	89
	By Mr. Becker	
	RECROSS-EXAMINATION	94
	By Mr. Fieman	
CHRIS SOGHOIAN	DIRECT EXAMINATION	99
	By Mr. Fieman	
	CROSS-EXAMINATION	120
	By Mr. Becker	
	REDIRECT EXAMINATION	128
	By Mr. Fieman	

EXHIBIT INDEX

EXHIBITS ADMITTED	PAGE
12A	57
12B	58
15	62
15B	63
13B	71
13A	91
1 - 9	97
A15 & A16	98

09:31:34AM 1 THE COURT: Good morning. This is
09:31:42AM 2 Cause No. 15-5351, United States versus Jay Michaud, who
09:31:46AM 3 is present in court with his attorneys, Mr. Fieman and
09:31:51AM 4 Ms. Sullivan. For the government, Mr. Becker.

09:32:03AM 5 MR. BECKER: Good morning, your Honor.

09:32:04AM 6 THE COURT: And Mr. Hamilton.

09:32:06AM 7 MR. HAMILTON: Good morning.

09:32:18AM 8 MR. BECKER: At counsel table is FBI Special Agent
09:32:26AM 9 Daniel Alfin.

09:32:26AM 10 THE COURT: Good morning. I put out a little
09:32:38AM 11 agenda for this proceeding. The first thing on the agenda
09:32:41AM 12 is arraignment on the superseding indictment. So let's
09:32:46AM 13 proceed with that first.

09:32:55AM 14 Mr. Michaud, have you received a copy of the
09:32:59AM 15 superseding indictment?

09:33:00AM 16 THE DEFENDANT: I have seen it, your Honor.

09:33:01AM 17 THE COURT: And you have had a chance to read that
09:33:03AM 18 and discuss it with your lawyers?

09:33:06AM 19 THE DEFENDANT: Yes, your Honor.

09:33:07AM 20 THE COURT: I think in prior proceedings we have
09:33:11AM 21 determined that your name is Jay Michaud, as it appears in
09:33:15AM 22 the caption of these documents; is that correct?

09:33:19AM 23 THE DEFENDANT: Yes, your Honor.

09:33:20AM 24 THE COURT: I think we also determined that you
09:33:23AM 25 can read and write English with no difficulty, and have

09:33:29AM 1 considerable secondary education, right?

09:33:32AM 2 THE DEFENDANT: Yes, your Honor.

09:33:33AM 3 THE COURT: And you understand that you have the
09:33:36AM 4 right to remain silent, and are not required to make any
09:33:40AM 5 statements about these matters?

09:33:41AM 6 THE DEFENDANT: I do, your Honor.

09:33:42AM 7 THE COURT: You also understand that you have the
09:33:45AM 8 right to counsel. And that has been provided in the
09:33:51AM 9 persons of Mr. Fieman and Ms. Sullivan. You have
09:33:57AM 10 conferred with them about this matter, the superseding
09:34:00AM 11 indictment?

09:34:00AM 12 THE DEFENDANT: Yes, your Honor.

09:34:01AM 13 THE COURT: And you understand that this
09:34:03AM 14 indictment supersedes and takes the place of the original
09:34:11AM 15 indictment filed in the case? Do you understand that?

09:34:13AM 16 THE DEFENDANT: I do now, your Honor.

09:34:15AM 17 THE COURT: Now, you have the right to have the
09:34:18AM 18 indictment read to you here in open court to be sure that
09:34:22AM 19 you understand it. Do you wish to have the indictment
09:34:25AM 20 read to you?

09:34:26AM 21 THE DEFENDANT: No, your Honor.

09:34:35AM 22 THE COURT: I believe the first two counts are the
09:34:45AM 23 same as in the original indictment; is that correct?

09:34:48AM 24 MR. HAMILTON: That's correct, your Honor.

09:34:51AM 25 THE COURT: You were advised of the penalties

09:34:55AM 1 possible in the event of conviction of those two charges?

09:35:01AM 2 THE DEFENDANT: Yes, your Honor.

09:35:01AM 3 THE COURT: As to the third charge, which is
09:35:04AM 4 Count 3, and is a new charge, what is the maximum penalty
09:35:09AM 5 that Mr. Michaud is facing for that charge?

09:35:13AM 6 MR. HAMILTON: Your Honor, the defendant faces a
09:35:22AM 7 minimum term of imprisonment of five years, and up to 20
09:35:25AM 8 years of imprisonment; a term of supervision following
09:35:29AM 9 release from prison of not less than five years, and up to
09:35:32AM 10 life; up to a \$250,000 fine; a \$100 mandatory special
09:35:42AM 11 assessment; and a \$5,000 penalty assessment if the court
09:35:46AM 12 finds the defendant is not indigent.

09:35:49AM 13 THE COURT: Do you understand those possible
09:35:52AM 14 penalties, Mr. Michaud?

09:35:54AM 15 THE DEFENDANT: Yes, your Honor.

09:35:56AM 16 THE COURT: And, counsel, are you satisfied that
09:35:58AM 17 Mr. Michaud is ready to enter a plea to these charges?

09:36:03AM 18 MS. SULLIVAN: We are, your Honor.

09:36:06AM 19 THE COURT: Mr. Michaud, in Count 1 you are
09:36:09AM 20 charged with possession of child pornography on or about
09:36:12AM 21 July 10th, 2015, at Vancouver, within this district. How
09:36:17AM 22 do you plead to that charge as it is set forth in the
09:36:19AM 23 superseding indictment?

09:36:20AM 24 THE DEFENDANT: Not guilty, your Honor.

09:36:22AM 25 THE COURT: In Count 2 you are charged with

09:36:24AM 1 receiving child pornography between February 21st and
09:36:31AM 2 March 2nd of last year within this district. How do you
09:36:35AM 3 plead to Count 2 as it is set forth in the superseding
09:36:39AM 4 indictment?

09:36:39AM 5 THE DEFENDANT: Not guilty, your Honor.

09:36:41AM 6 THE COURT: And in Count 3 you are charged with
09:36:44AM 7 receipt of child pornography on or about June 18th of last
09:36:48AM 8 year, at Vancouver, within this district. How do you
09:36:52AM 9 plead to Count 3 as it is set forth in the superseding
09:36:56AM 10 indictment?

09:36:56AM 11 THE DEFENDANT: Not guilty, your Honor.

09:36:58AM 12 THE COURT: All right. The pleas will be entered.
09:37:05AM 13 We will turn our attention to other matters.

09:37:08AM 14 MS. SULLIVAN: Your Honor, before we turn our
09:37:11AM 15 attention to that, in connection with the arraignment we
09:37:14AM 16 had asked that Mr. Michaud's bond conditions be reduced to
09:37:20AM 17 a level where he is on electronic monitoring, but just on
09:37:24AM 18 a curfew. I understand that Pretrial Services is prepared
09:37:28AM 19 to do that and is in agreement with that, and we would ask
09:37:32AM 20 that the bond condition be modified accordingly.

09:37:36AM 21 THE COURT: I have not heard from Pretrial
09:37:39AM 22 Services on this.

09:37:50AM 23 PRETRIAL SERVICES OFFICER: Good morning, your
09:37:54AM 24 Honor. I am Jamie Parkhurst with Pretrial Services.
09:37:58AM 25 Mr. Michaud has been on supervision with our office since

09:38:00AM 1 he was placed on bond. He has been in compliance. He did
09:38:03AM 2 have one violation, where we recommended no action be
09:38:06AM 3 taken by the court. At this time we do feel that it is
09:38:10AM 4 appropriate for him to be moved to a curfew.

09:38:13AM 5 THE COURT: Mr. Becker or --

09:38:20AM 6 MR. HAMILTON: Your Honor, the government has no
09:38:22AM 7 objection to that.

09:38:23AM 8 THE COURT: All right. The motion then will be
09:38:25AM 9 granted and the release bond will be modified as requested
09:38:37AM 10 in the defendant's motion.

09:38:39AM 11 MS. SULLIVAN: Thank you, your Honor.

09:38:48AM 12 THE COURT: I guess the next matter is the motion
09:38:52AM 13 to compel that is pending. I read the response filed by
09:39:11AM 14 the government. They also asked for an order granting the
09:39:18AM 15 request to file a response in excess of 12 pages. Since I
09:39:23AM 16 have already read 21 pages, I will grant that motion.

09:39:34AM 17 But I must say, having read all of your briefs twice
09:39:38AM 18 now, and some parts of your briefs more than twice, I wish
09:39:47AM 19 that I had not granted the first motion to compel or any
09:39:50AM 20 of the ones since. Strike that. Not motion to compel.
09:39:56AM 21 The motion to exceed page limits. There is a lot of
09:40:03AM 22 excess talk in all of your pleadings that just is not
09:40:12AM 23 necessary. Be that as it may, I will grant the motion for
09:40:21AM 24 excess pages in regards to the government's motion to
09:40:29AM 25 compel.

09:40:30AM 1 Now, I read those pleadings. Everybody seemed to want
09:40:36AM 2 more time on that issue for one reason or another. I
09:40:44AM 3 don't know if you want to address that in any way today or
09:40:50AM 4 not, Mr. Fieman. The government says there is no
09:40:57AM 5 relevance or materiality --

09:41:00AM 6 MR. FIEMAN: Your Honor, I have only been able to
09:41:02AM 7 briefly skim the 21 pages since it came in. I can only
09:41:06AM 8 say, based on my preliminary survey, there is some
09:41:09AM 9 substantial disputes. We would want time to respond, as
09:41:11AM 10 briefly as possible.

09:41:14AM 11 But as I indicated in my initial motion to compel,
09:41:18AM 12 they have assured us that they are not withholding any
09:41:21AM 13 information that is relevant to the pending motions. But
09:41:25AM 14 as indicated, also in our motion, if we do move into the
09:41:29AM 15 trial phase, as the case proceeds after this hearing,
09:41:32AM 16 there are now separate trial-related issues. And we would
09:41:35AM 17 want the opportunity to respond to that and address some
09:41:38AM 18 of the claims that I very briefly saw in the government's
09:41:42AM 19 filing late last night.

09:41:46AM 20 Your Honor, I would defer to the court on how long --
09:41:49AM 21 That is at least a week to do that. Mostly because in
09:41:53AM 22 preparation for this hearing we have a lot of things
09:41:55AM 23 backed up next week in terms of my other clients' needs.
09:42:00AM 24 But any reasonable amount of time, we can file a response.

09:42:02AM 25 I can tell your Honor this will spill over into chain

09:42:08AM 1 of custody and Daubert issues that will probably be raised
09:42:12AM 2 separately. It might be more efficient, once we have
09:42:15AM 3 talked about some scheduling issues that the government
09:42:17AM 4 has raised with me in terms of the trial and Mr. Becker's
09:42:20AM 5 availability, possibly to confer after the hearing today,
09:42:25AM 6 if the case proceeds, and submit a proposed schedule to
09:42:29AM 7 the court.

09:42:35AM 8 THE COURT: Just exactly what are you asking for?

09:42:39AM 9 MR. FIEMAN: Your Honor, we are asking for what we
09:42:41AM 10 asked for from the beginning, and we thought we were
09:42:44AM 11 getting, which is the --

09:42:45AM 12 THE COURT: I'm sorry. I am having a hard time
09:42:45AM 13 hearing you. Why don't you raise that whole thing up.
09:42:49AM 14 Hit the switch down by your knee.

09:43:00AM 15 MR. FIEMAN: Is that better, your Honor?

09:43:01AM 16 THE COURT: Yes.

09:43:03AM 17 MR. FIEMAN: Your Honor, we are asking for what we
09:43:06AM 18 thought they agreed to, which is the NIT programming code.
09:43:09AM 19 As indicated, we got a piece of it.

09:43:12AM 20 They have a different understanding of our agreement.
09:43:15AM 21 That's fine. I don't want to go backwards and have a he
09:43:20AM 22 said/she said contest, but the parts that are missing are
09:43:22AM 23 important for our trial preparation.

09:43:25AM 24 THE COURT: If I understand what you're saying,
09:43:26AM 25 you want a little more time to respond?

09:43:29AM 1 MR. FIEMAN: Yes, your Honor. Definitely that.
09:43:31AM 2 That's where I started. It is just a question of how much
09:43:33AM 3 time?

09:43:33AM 4 THE COURT: That's what I am asking you, how much
09:43:35AM 5 time.

09:43:36AM 6 MR. FIEMAN: At least a week, your Honor. I would
09:43:39AM 7 ask for a week from Monday, actually, realistically.

09:43:46AM 8 THE COURT: Mr. Becker.

09:43:47AM 9 MR. BECKER: Your Honor, as to the scheduling of
09:44:00AM 10 the motion to compel, we don't have an objection to the
09:44:03AM 11 defense having that time that is requested to respond. We
09:44:08AM 12 certainly -- We did think -- Obviously, as you have seen
09:44:12AM 13 in our pleading, we do believe that we have provided
09:44:15AM 14 sufficient information, and we don't believe the request
09:44:17AM 15 for additional information is material. And we maintain
09:44:20AM 16 that position.

09:44:22AM 17 We certainly -- Over the last week it seemed like the
09:44:25AM 18 defense thought that this issue was pertinent to this
09:44:27AM 19 hearing, and obviously asked for an expedited hearing, and
09:44:30AM 20 we are on different footing now. That is what it is. We
09:44:34AM 21 did respond. I apologize for the length, your Honor. We
09:44:37AM 22 have obviously been -- There have been a lot of issues we
09:44:40AM 23 have been dealing with this week in getting ready for this
09:44:44AM 24 hearing.

09:44:44AM 25 THE COURT: It takes more time to write a short

09:44:46AM 1 brief than a long one.

09:44:48AM 2 MR. BECKER: Sometimes, your Honor. We don't
09:44:50AM 3 object to the additional time. I certainly do want to
09:44:52AM 4 flag for the court, as we flagged in our response, in the
09:44:55AM 5 event that the court were to find that there are material
09:44:58AM 6 issues involved, that we are requesting an ex parte
09:45:03AM 7 in camera hearing in order to present further information
09:45:06AM 8 pertinent to the law enforcement privilege.

09:45:09AM 9 As long as the court will at least hear that request
09:45:11AM 10 on this schedule, we don't object to the defense having
09:45:15AM 11 more time to respond. I think we can confer after today's
09:45:20AM 12 hearing in terms of other scheduling matters. We have had
09:45:23AM 13 preliminary conversations about a potential continuance of
09:45:25AM 14 the trial date in light of the numerous issues -- the
09:45:29AM 15 pretrial issues which still need to be resolved. And I
09:45:31AM 16 think the parties have an eye towards being able to agree
09:45:35AM 17 on that, in order that the court can decide all of the
09:45:38AM 18 pretrial matters that it needs to decide.

09:45:41AM 19 THE COURT: I think the first thing here is the
09:45:44AM 20 scheduling on this motion. It is appropriate to set a
09:45:50AM 21 response for a week from Monday -- a reply, that is. It
09:45:56AM 22 appears to me that the government is throwing the gauntlet
09:45:59AM 23 down on the question of relevance and materiality of the
09:46:04AM 24 requested information. We will note it up for that, I
09:46:25AM 25 guess, the Tuesday following that. At that point we will

09:46:28AM 1 have to decide what other hearings, if any, may be
09:46:31AM 2 necessary on that subject.

09:46:34AM 3 I am very reluctant to have an in camera hearing. I
09:46:40AM 4 know that that's appropriate in some circumstances. It
09:46:46AM 5 challenges due process. I would rather deal with that
09:46:55AM 6 insofar as we can without the necessity of any hearing or
09:47:01AM 7 information that is kept from the defendant.

09:47:04AM 8 MR. BECKER: We certainly understand and respect
09:47:06AM 9 that, your Honor. We don't take making a request like
09:47:09AM 10 that lightly at all. Certainly we have set forth
09:47:12AM 11 substantial arguments that have been made openly and will
09:47:16AM 12 be made openly. That said, we have also set forth
09:47:19AM 13 substantial authority within the Ninth Circuit for the
09:47:22AM 14 resolution of issues, such as this, in part via ex parte
09:47:26AM 15 in camera hearing by the court as a part of the resolution
09:47:30AM 16 of the issues.

09:47:32AM 17 THE COURT: If that's necessary we will deal with
09:47:35AM 18 that after we get the pleadings closed.

09:47:38AM 19 MR. BECKER: Your Honor, in terms of the Tuesday
09:47:40AM 20 that your Honor mentioned for scheduling, I am not sure
09:47:42AM 21 what day that falls on. I do have some trial -- some
09:47:46AM 22 other trial availability and needs in other districts. I
09:47:51AM 23 am just not sure what date your Honor has suggested, that
09:47:53AM 24 Tuesday.

09:47:54AM 25 THE CLERK: That would be February 2nd.

09:48:03AM 1 THE COURT: Okay. When I get that we will take a
09:48:06AM 2 look at it and decide the future of the motion to compel.

09:48:14AM 3 MR. BECKER: Thank you, your Honor.

09:48:22AM 4 THE COURT: You want to be heard further on your
09:48:24AM 5 request for a Franks hearing.

09:48:30AM 6 MR. FIEMAN: Your Honor, as set forth in our
09:48:35AM 7 pleadings, our position is that, given the issues relating
09:48:41AM 8 to the four corners of the warrant, the undisputed facts,
09:48:44AM 9 and the exhibits that have been presented to the court, we
09:48:50AM 10 have definitely made a showing for the Franks hearing. I
09:48:52AM 11 will briefly summarize what that is in a moment, plus some
09:48:55AM 12 new information that has come to light.

09:48:58AM 13 But the Franks hearing, as indicated in my pleadings,
09:49:01AM 14 would be rendered moot based upon what we believe are
09:49:04AM 15 dispositive issues that are already before the court.

09:49:09AM 16 But addressing your question directly, we do believe
09:49:12AM 17 we have met our burden of showing that there is a Franks
09:49:15AM 18 issue. And that is directed primarily -- although there
09:49:19AM 19 are a host of issues that we flagged, primarily to two
09:49:23AM 20 things: That is, first of all, intentionally false or
09:49:29AM 21 misleading statements about the location to be searched,
09:49:33AM 22 leading to a warrant on its face, as limited to the
09:49:36AM 23 Eastern District of Virginia, while the warrant was in
09:49:40AM 24 fact executed, in Mr. Michaud's case, in Washington.

09:49:43AM 25 The second core Franks issues is intentionally or

09:49:47AM 1 recklessly misleading the court or failing -- recklessly
09:49:52AM 2 failing to verify the homepage information. And we
09:49:55AM 3 believe this is critical, because it goes to the heart of
09:49:58AM 4 the probable cause.

09:50:00AM 5 The court is aware of Gourde and the other cases. The
09:50:04AM 6 government has essentially hung its probable cause
09:50:06AM 7 argument on the claim that this would be immediately
09:50:11AM 8 apparent as a dedicated child pornography site to even a
09:50:15AM 9 first time visitor, because that's all that matters
09:50:18AM 10 really, is what's on the homepage, because the warrant
09:50:20AM 11 authorized the search as of logging in on the homepage.

09:50:24AM 12 Now, your Honor, I don't believe in fact that there is
09:50:28AM 13 any testimony even required to resolve that issue in our
09:50:32AM 14 favor. And I will tell you why. Because there are only
09:50:34AM 15 two possible answers that the agent could give. One is he
09:50:37AM 16 did not check the homepage after he viewed it, I believe,
09:50:42AM 17 on February 18th. The site was seized on the 19th, the
09:50:48AM 18 warrant was submitted on the 20th. Let's take that at
09:50:51AM 19 face value. We now know from government exhibits that
09:50:54AM 20 they were aware at the time of the execution of the search
09:50:56AM 21 warrant in Naples, Florida, on the 19th, when they seized
09:51:02AM 22 the website, that the logo had changed.

09:51:09AM 23 And really it comes down to that issue of whether the
09:51:11AM 24 pictures that were on the banner as of February 3rd were
09:51:16AM 25 lascivious, and therefore qualified -- clearly indicated

09:51:22AM 1 pornography. That point is debatable in itself. But it
09:51:25AM 2 is a secondary point.

09:51:26AM 3 The point is, when you take the homepage at face
09:51:29AM 4 value, as it was at the time the warrant was issued, it is
09:51:32AM 5 clearly not advertising itself as a child pornography
09:51:37AM 6 site. There is no lascivious pictures. It doesn't
09:51:41AM 7 indicate in any way it is anything other than a chat or an
09:51:44AM 8 erotic content site.

09:51:46AM 9 Now, as I said, the officer could say one of two
09:51:50AM 10 things: Either he didn't check after the site was seized,
09:51:53AM 11 which under the circumstances, with a dynamic website --
09:51:57AM 12 The fact that the FBI in fact had control of the site as
09:52:01AM 13 of the 19th, the day before the warrant application, we
09:52:05AM 14 submit by any common sense measure that is a reckless
09:52:08AM 15 failure to verify, particularly when there are claims
09:52:11AM 16 about the agent's experience with internet investigations
09:52:13AM 17 and the dynamic nature of websites.

09:52:16AM 18 The other alternative is that he did know that the
09:52:19AM 19 logo had changed, in which case I don't know if anything
09:52:23AM 20 more would need to be said at all.

09:52:25AM 21 So, your Honor, we believe we have amply established
09:52:28AM 22 the need for a Franks hearing in terms of the Franks
09:52:30AM 23 issues in evidence. We do not believe the court needs to
09:52:33AM 24 reach that because we believe this case is resolved on the
09:52:37AM 25 four corners of the warrant application.

09:52:41AM 1 THE COURT: To justify a separate Franks hearing
09:52:47AM 2 there has to be a substantial preliminary showing that a
09:52:51AM 3 false statement knowingly and intentionally, or with
09:52:54AM 4 reckless disregard for the truth, was included by the
09:53:00AM 5 affiant; and, also, that the alleged false statement is
09:53:09AM 6 necessary to a finding of probable cause.

09:53:13AM 7 I don't think that preliminary showing has been made
09:53:14AM 8 here. I think the issues that you raise are part of the
09:53:19AM 9 other issues in the case regarding suppression and
09:53:23AM 10 sufficiency of the application, and they can fairly be
09:53:29AM 11 reached without a separate Franks hearing. I think there
09:53:35AM 12 is just not the necessity for that hearing. I don't think
09:53:41AM 13 the showing is sufficient under that standard.

09:53:44AM 14 MR. FIEMAN: Your Honor, just to understand you,
09:53:46AM 15 we are still able to explore those factual --

09:53:47AM 16 THE COURT: I'm sorry. What?

09:53:50AM 17 MR. FIEMAN: Your Honor, just so I'm clear, we
09:53:53AM 18 will still be able to address the evidence related to --

09:53:55AM 19 THE COURT: Sure.

09:53:57AM 20 MR. FIEMAN: -- all of those probable cause
09:54:00AM 21 application issues --

09:54:01AM 22 THE COURT: It is all part of the motion to
09:54:02AM 23 suppress.

09:54:03AM 24 MR. FIEMAN: Thank you, your Honor.

09:54:04AM 25 THE COURT: Or motions to suppress. The next

09:54:11AM 1 matter is the motion to dismiss based on outrageous
09:54:25AM 2 government conduct. I would like to hear anything you
09:54:37AM 3 want to say about that.

09:54:38AM 4 MR. FIEMAN: Thank you, your Honor. And I do have
09:54:42AM 5 a few things I want to say about that. Because with -- as
09:54:45AM 6 indicated in our initial motion to dismiss, the dismissal
09:54:52AM 7 motion also includes -- it says if there is a lesser
09:54:57AM 8 remedy that accomplishes the same deterrent purposes, the
09:55:00AM 9 court should take that into account.

09:55:03AM 10 Again, we are kind of overlapping with some of the
09:55:06AM 11 suppression issues.

09:55:07AM 12 I just want to very briefly state where we see this
09:55:09AM 13 case to be and the very specific issues that we think are
09:55:14AM 14 dispositive, either in terms of dismissal or finding
09:55:19AM 15 grounds for dismissal and choosing suppression as an
09:55:26AM 16 appropriate remedy.

09:55:28AM 17 Let me just summarize what we see this case to be
09:55:31AM 18 about, your Honor. In some ways it comes down to a
09:55:35AM 19 constitutional line to the sand. The government has
09:55:41AM 20 legitimate challenges trying to investigate internet
09:55:46AM 21 crime. We do not dispute that.

09:55:49AM 22 What we do dispute is whether or not the government
09:55:53AM 23 can unilateral determine the scope and extent of its
09:55:57AM 24 investigatory powers without judicial oversight and in
09:56:02AM 25 defiance of the laws, Rule 41 in particular, and the

09:56:07AM 1 restrictions on illegal investigations that are on the
09:56:11AM 2 books.

09:56:12AM 3 Now, they can advocate for changes. They can seek
09:56:17AM 4 warrants that allow them to extend their powers. But what
09:56:20AM 5 we believe they cannot do is engage in this kind of
09:56:26AM 6 gamesmanship with judicial oversight that has been
09:56:30AM 7 evidenced not only throughout this case but in a pattern
09:56:34AM 8 of these technology cases that is leading, we think, to a
09:56:37AM 9 very substantial Fourth Amendment and privacy rights
09:56:40AM 10 crisis.

09:56:41AM 11 It is often unfortunate that these constitutional
09:56:43AM 12 issues are presented in the court in the context of the
09:56:47AM 13 type of allegations that are made in this case. If we
09:56:50AM 14 were dealing with bank fraud or white collar defendants
09:56:53AM 15 who had their private computers hacked, there is a
09:56:57AM 16 different momentum. We recognize that. But Mr. Michaud
09:57:00AM 17 stands here -- This is his case. It is not about any
09:57:02AM 18 other cases they have charged. He stands here with the
09:57:05AM 19 presumption of innocence as a man who has been subjected
09:57:08AM 20 to a Washington search on the basis of an invalid Virginia
09:57:12AM 21 warrant. That is the core of our claim.

09:57:16AM 22 Now, your Honor, I want to zero in on one issue that
09:57:20AM 23 goes to the heart of this dismissal, and all of the
09:57:23AM 24 issues. It is the one issue we raised -- And it is front
09:57:26AM 25 and center. In all the reams of paper the court has waded

09:57:30AM 1 through, the government has not once responded to it. And
09:57:35AM 2 this is this: They sought a warrant from the Eastern
09:57:40AM 3 District of Virginia. They got authority to search
09:57:43AM 4 computers, persons, and property in the Eastern District
09:57:46AM 5 of Virginia. They drafted that warrant. They changed the
09:57:48AM 6 face of their warrants. They used to say in Nebraska and
09:57:52AM 7 elsewhere, Colorado and elsewhere. And once they
09:57:55AM 8 realized, after Judge Smith's decision and their own
09:57:58AM 9 internal policies, that Rule 41 simply did not allow that,
09:58:01AM 10 they simply edited the warrant.

09:58:03AM 11 Now, taking that warrant at face value -- And this is
09:58:05AM 12 why we have been really hammering this, your Honor,
09:58:09AM 13 because it is a brick and mortar issue. There is no
09:58:11AM 14 dispute at this point that the search occurred on
09:58:14AM 15 Mr. Michaud in his home in Washington.

09:58:17AM 16 Now, imagine if the government had gotten a warrant in
09:58:22AM 17 the Eastern District of Virginia to search multiple --
09:58:25AM 18 hundreds of thousands of houses in the Eastern District of
09:58:28AM 19 Virginia, and they then decided that they were going to
09:58:31AM 20 get in that car, drive across country, go into
09:58:34AM 21 Mr. Michaud's home, extract information from his computer
09:58:39AM 22 on the basis of that Virginia warrant. It would be a
09:58:42AM 23 non-starter. It would be a non-starter. It would be a
09:58:44AM 24 non-starter because it violates what is the plain language
09:58:49AM 25 of the warrant itself, and it is in violation of the

09:58:52AM 1 execution limits that were in that warrant.

09:58:55AM 2 So what I am asking the court to do, in some sense, is
09:58:58AM 3 to set aside all of these technology issues, all of this
09:59:02AM 4 back and forth about who was truthful, who was not
09:59:06AM 5 truthful, and look at the face of the warrant. Because if
09:59:09AM 6 this were any other case, a drug bust case, a bank fraud
09:59:13AM 7 case, we would be over now.

09:59:18AM 8 And wrapped up in that, your Honor, is this
09:59:24AM 9 government -- the government's argument that somehow all
09:59:26AM 10 of this was necessary.

09:59:28AM 11 THE COURT: All what?

09:59:30AM 12 MR. FIEMAN: All of what they did in terms of
09:59:31AM 13 obtaining the warrant and executing the NITs was
09:59:35AM 14 necessary, that they had no alternatives. That is a false
09:59:37AM 15 statement.

09:59:38AM 16 This warrant authorized them to deploy NITs at the
09:59:44AM 17 time people logged into the home site. They did not need
09:59:48AM 18 to allow access to actual pornography on the site.

09:59:51AM 19 We have learned as of last night that in fact this is
09:59:53AM 20 not the first time the government has run a child
09:59:55AM 21 pornography site. It has apparently been done in secret
09:59:58AM 22 several times before, and we have received confirmation of
10:00:01AM 23 that.

10:00:01AM 24 This is a very troubling aspect of the case. Not only
10:00:04AM 25 are they not being candid with the court in terms of

10:00:07AM 1 allowing magistrates to supervise, or limit, or simply
10:00:13AM 2 exercise full review of the warrant applications, they are
10:00:16AM 3 now not even disclosing to the courts in all of these
10:00:20AM 4 cases that they are planning to continue the distribution
10:00:23AM 5 of child pornography as part of their investigations.

10:00:25AM 6 We consider that outrageous, because even if there is
10:00:29AM 7 a legitimate argument for doing that as an investigatory
10:00:32AM 8 need, which is not true, judges need to be able to decide
10:00:38AM 9 if it is appropriate. And, frankly, we believe it is
10:00:43AM 10 appalling.

10:00:46AM 11 Now, your Honor, as I also indicated, wrapped up with
10:00:52AM 12 this dismissal motion is the core issue of probable cause,
10:00:56AM 13 because we do think it is outrageous that when presenting
10:01:00AM 14 such a sweeping warrant to a magistrate, that in this case
10:01:05AM 15 authorized up to 100,000 searches, that they were not
10:01:11AM 16 candid or responsible in terms of the key facts in that
10:01:16AM 17 probable cause assessment, which was the homepage.

10:01:20AM 18 So what you ended up with is a warrant that allowed
10:01:25AM 19 tens of thousands, possibly hundreds of thousands, of
10:01:29AM 20 searches anywhere in the world based on people signing
10:01:33AM 21 into a website that does not even advertise itself as
10:01:36AM 22 having illegal content. And, frankly, the scope of that
10:01:41AM 23 is unprecedented.

10:01:43AM 24 And we haven't even gotten to the Rule 41 violations,
10:01:49AM 25 your Honor, which I will not address, because that is a

10:01:51AM 1 separate matter.

10:01:52AM 2 And all this time, while this is going on, the FBI
10:01:56AM 3 itself is aiding and abetting the uploading and
10:02:00AM 4 distribution of massive amounts of child pornography. I
10:02:05AM 5 don't want to sound at all self-righteous about this, your
10:02:11AM 6 Honor, because I understand the nuances of criminal cases,
10:02:13AM 7 and I defend people who are charged with distributing or
10:02:18AM 8 possessing child pornography, most obviously. But those
10:02:22AM 9 people face criminal charges. All we are asking is that
10:02:26AM 10 the government face judicial oversight.

10:02:32AM 11 So, your Honor, we believe that we have strong grounds
10:02:36AM 12 for dismissal of the indictment. We invite the court to
10:02:42AM 13 choose the lesser remedy that courts have approved for
10:02:46AM 14 outrageous government conduct, of suppression. We
10:02:50AM 15 believe, your Honor, that this is a pivotal moment for
10:02:55AM 16 privacy and constitutional rights in the digital age.
10:02:59AM 17 That is a lot for Mr. Michaud to bear, and we don't want
10:03:03AM 18 to lose sight of the man that is sitting here, and the
10:03:06AM 19 court has had a chance to assess.

10:03:08AM 20 But the core of it is this: Even if the government
10:03:11AM 21 believes that it was perfectly allowed to do what it did,
10:03:16AM 22 then why did they not tell Judge Buchanan what they were
10:03:21AM 23 doing about running a child pornography site? Why didn't
10:03:23AM 24 they draft a warrant that clearly stated that they would
10:03:27AM 25 execute it outside the Eastern District of Virginia? Why

10:03:32AM 1 take those steps if this is all legal and appropriate?

10:03:36AM 2 Your Honor, I come back to the same argument. I
10:03:39AM 3 believe the court can dispose of all these issues based
10:03:42AM 4 simply on the face of the warrant, the government's
10:03:44AM 5 failure to explain the discrepancy between the warrant
10:03:47AM 6 itself and the scope that they claim allowed them for the
10:03:53AM 7 searches, and the discrepancy also, your Honor, between
10:03:56AM 8 the fact that now we know up to 100,000 people accessed
10:04:01AM 9 this supposedly dedicated child pornography site, and yet
10:04:05AM 10 we see no evidence, when we look at the homepage itself,
10:04:10AM 11 that was not presented to the magistrate in the Eastern
10:04:13AM 12 District of Virginia accurately, that in fact this is a
10:04:16AM 13 very ambiguous location. Thank you, your Honor.

10:04:43AM 14 MR. BECKER: Your Honor, I would start by, again,
10:05:00AM 15 bringing us back to, as I think I have before here, the
10:05:05AM 16 legal standards and principles that apply. Because what
10:05:09AM 17 you don't hear in the defendant's argument are any
10:05:13AM 18 applications of them whatsoever.

10:05:15AM 19 And there is a standard that the Ninth Circuit has
10:05:18AM 20 laid out in determining whether or not government conduct
10:05:22AM 21 is quote-unquote outrageous. It is an extremely high bar.
10:05:30AM 22 We believe there is no question that that bar is nowhere
10:05:32AM 23 near met in this case.

10:05:35AM 24 We are dealing with actions by law enforcement that
10:05:41AM 25 were necessitated by the actions of the offenders choosing

10:05:44AM 1 to use, and in fact misuse, technology in order to hide
10:05:49AM 2 their identity while they sought to exploit and abuse
10:05:53AM 3 children online.

10:05:55AM 4 And law enforcement responded to that enormous
10:05:58AM 5 problem -- The enormity of that problem, your Honor, is
10:06:02AM 6 borne out by the active use of this site. The fact that
10:06:07AM 7 there were so many thousands of users and so much child
10:06:10AM 8 pornography being distributed long before law enforcement
10:06:15AM 9 ever seized it is an indication of the scope of the
10:06:17AM 10 problem that law enforcement faced.

10:06:21AM 11 In the face of that, what actions did law enforcement
10:06:24AM 12 take? They went to the court. I can't figure out what
10:06:29AM 13 warrant the defense -- what NIT warrant the defense is
10:06:33AM 14 reading and what Title III application the defense is
10:06:36AM 15 reading when they say that the government, the FBI, took
10:06:41AM 16 these actions without judicial oversight. That is simply
10:06:45AM 17 wrong. It is incorrect.

10:06:49AM 18 The affidavit in support of the network investigative
10:06:52AM 19 technique unmistakably advised the magistrate that the
10:06:57AM 20 child pornography website involved here was going to
10:07:00AM 21 remain operating at a government facility in order for
10:07:04AM 22 that then court-authorized investigative technique to be
10:07:09AM 23 deployed.

10:07:09AM 24 That warrant articulated to Magistrate Judge Buchanan
10:07:14AM 25 why that technique was necessary, because we were dealing

1 with a website that operated on the anonymous Tor network.
2 That changes the game in terms of what law enforcement has
3 available to them in order to identify users. That is
4 laid out in detail in the NIT warrant affidavit. And no
5 reasonable reading of that affidavit would show that the
6 magistrate would not have known that the site was going to
7 continue to operate at a government facility. It is
8 directly stated.

9 The Title III affidavit and application approved by a
10 United States District Court judge also articulated that
11 the website would remain operating at a government
12 facility, and that the United States, the FBI, was going
13 to seek and obtain authorization to deploy a network
14 investigative technique on its users. It discussed the
15 reasons why, again, the necessity of the site having to
16 remain operating in order to deploy that sort of
17 technique.

18 So I just don't understand the argument that there was
19 not judicial oversight involved here when the actions that
20 law enforcement took were judicially approved. That is
21 judicial oversight.

22 So bringing us back to the standards here, your Honor,
23 in terms of the dismissal issue: Again, extremely high
24 standard according to the Ninth Circuit. So high in fact
25 that the Ninth Circuit has consistently refused to find

1 outrageous government conduct where the government used
2 so-called reverse stings; that is, where there was no
3 criminal enterprise that was going on, the government
4 created or came up with sort of a fake scheme in which
5 defendants participated and were charged. Even in those
6 sorts of scenarios, which is vastly different than this
7 scenario, the Ninth Circuit has not found outrageous
8 conduct.

9 But the standards here, as laid down by the circuit,
10 involve a six-factor analysis. It involves the known
11 criminal characteristics of the defendant; whether there
12 was individualized suspicion of the defendant; the
13 government's role in creating, if at all, the crime of
14 conviction; the government's encouragement, if at all, of
15 the defendant to commit the particular conduct; the nature
16 of the government's participation in the conduct; and the
17 nature of the crime being pursued; the necessity for the
18 actions taken in light of the criminal enterprise at
19 issue.

20 Your Honor, as we have argued in our briefing, all of
21 those factors weigh heavily in favor of the government's
22 conduct being reasonable in this case -- in this
23 investigation in response to the particular concerns
24 involved. And the crime does matter. It is not -- it is
25 important that we are talking about the online sexual

1 exploitation of children. That does substantively matter
2 in terms of the public safety and interests at stake. It
3 does matter that these offenders were acting online,
4 misusing a Tor technology for their own criminal aims,
5 making it extremely difficult for them to be identified.
6 That absolutely matters.

7 The suggestion that somehow the standards would be
8 different or apply differently because of the subject
9 matter of the crime -- I think the defense sort of wants
10 to imply that because this crime involves children that
11 somehow we will give more latitude to the government in
12 some ways. And that is certainly not -- I don't believe
13 that is the case at all.

14 The fact that the crimes do involve children, though,
15 means there is a compelling interest and need to
16 investigate the perpetrators, to identify them and to
17 apprehend them, not just to shut down the facilities
18 through which they facilitate and distribute unlawful
19 contraband.

20 I would like to go through on a more individual basis
21 the particular factors, your Honor. The first two
22 characteristics, the known criminal characteristics of
23 users, individualized suspicion of the defendant:
24 Certainly at the outset of the investigation here the
25 government wasn't aware of any conduct by Michaud. That

1 is because he was acting anonymously on the Tor network.
2 We know that he joined this website long before the
3 government ever took actions to take it over.

4 But there was certainly good reason to suspect the
5 criminal users of this website of engaging in the
6 trafficking of child pornography: Access, distribution,
7 and receipt. And that is borne out by the investigation,
8 the way the site works.

9 As the defense concedes -- at least in the context of
10 their dismissal motions, the defense concedes and in fact
11 affirmatively argues that this website facilitated child
12 pornography on a massive scale. It is only when they are
13 on the suppression side of things that they want to shift
14 their argument to this website being merely a discussion
15 forum and nothing else. Well, they can't have it both
16 ways, your Honor.

17 The fact is, this was a child pornography website,
18 through which substantial amounts of child pornography
19 were trafficked and distributed long before the government
20 took specific actions against the site.

21 And so the individual -- the users of this site,
22 clearly legitimate targets of government investigation.
23 And that had nothing to do with anything the government
24 created in terms of the criminal scheme. That was those
25 users' criminal scheme.

10:13:09AM 1 That leads into the next factor, your Honor. And that
10:13:13AM 2 is, again, did the government play a role in the creation
10:13:16AM 3 of the crime in which this defendant, Mr. Michaud, is
10:13:20AM 4 accused? Here, and the law bears this out, the government
10:13:26AM 5 merely attached itself to one that was already established
10:13:29AM 6 and ongoing. That weighs against any finding of
10:13:32AM 7 outrageous government conduct. The United States, the
10:13:35AM 8 FBI, didn't create this website. It was created by its
10:13:39AM 9 users and its administrators, and existed and
10:13:44AM 10 substantially distributed child pornography long before
10:13:46AM 11 the government ever took it over in an effort to actually
10:13:49AM 12 identify its criminal users.

10:13:52AM 13 Did the government encourage the defendant to
10:13:56AM 14 participate in the crimes at issue? We know that is
10:13:59AM 15 absolutely not the case. The defendant, his user account
10:14:05AM 16 Pewter, joined the website on October 31st, 2014, long
10:14:09AM 17 before law enforcement ever received the website. The
10:14:13AM 18 government had nothing to do with his independent decision
10:14:15AM 19 to associate himself with this criminal enterprise.

10:14:18AM 20 The nature of the government's participation, and was
10:14:22AM 21 it responsible -- Was the nature of what the government
10:14:24AM 22 did responsible for Michaud's crimes? Again, weighs
10:14:29AM 23 against a finding of outrageous conduct here.

10:14:31AM 24 Did the government act as a partner in the criminal
10:14:34AM 25 activity, or more of an observer in the defendant's

10:14:38AM 1 criminal conduct? Well, here, again, the site was already
10:14:42AM 2 operating, had operated for six months. For 14 brief days
10:14:47AM 3 the government allowed it to continue to operate on a
10:14:49AM 4 government server in order to take specific
10:14:52AM 5 court-authorized actions to attempt to identify users and
10:14:55AM 6 monitor user communications.

10:14:58AM 7 The government, the FBI, did not post any links,
10:15:03AM 8 videos -- any images, videos, or links to images, or
10:15:07AM 9 videos of child pornography. The FBI conducted
10:15:11AM 10 court-authorized monitoring, conducted court-authorized
10:15:15AM 11 deployment of the NIT in order to collect information that
10:15:18AM 12 would help identify the people who were actually
10:15:20AM 13 perpetrating the crimes.

10:15:22AM 14 Another factor in this part is whether the defendant
10:15:26AM 15 would have the technical expertise or resources necessary
10:15:31AM 16 to commit such a crime without the government's
10:15:34AM 17 intervention. Undoubtedly that is the case with
10:15:37AM 18 Mr. Michaud. He is charged with counts of possessing and
10:15:39AM 19 receiving child pornography that have nothing to do with
10:15:42AM 20 the website at issue, based on images that were found on
10:15:45AM 21 his devices that were seized from his home, or pursuant to
10:15:50AM 22 other residential search warrants. He clearly had the
10:15:54AM 23 technical ability to navigate Tor and get to this website,
10:15:58AM 24 because he joined it long before law enforcement took it
10:16:02AM 25 over.

10:16:02AM 1 This is another area where the defense focuses on --
10:16:06AM 2 away from Mr. Michaud, the actual defendant here in this
10:16:09AM 3 case, and more on the other users of the website. This
10:16:12AM 4 case is about Mr. Michaud, what is he charged with, what
10:16:16AM 5 was his conduct, and was the government responsible for
10:16:20AM 6 that conduct? And the answer is just no. There wasn't
10:16:23AM 7 any direct contact with Mr. Michaud during the operation.
10:16:31AM 8 The defense doesn't allege that, and neither does the
10:16:34AM 9 government.

10:16:34AM 10 The fact is he made an independent choice to associate
10:16:37AM 11 himself with a criminal enterprise that was later taken
10:16:39AM 12 over. And because the government did that, we eventually
10:16:43AM 13 got information to help identify him, and nothing more.

10:16:47AM 14 So that comes around to the last factor, which is the
10:16:50AM 15 need for the investigative technique used in light of the
10:16:53AM 16 challenges of investigating and prosecuting the type of
10:16:56AM 17 crime being investigated. This factor, your Honor,
10:16:59AM 18 absolutely weighs in favor of the government's conduct
10:17:03AM 19 being reasonable in light of the circumstances, the
10:17:08AM 20 government going to courts -- not just one court, but
10:17:11AM 21 courts, for approval for the investigative technique that
10:17:15AM 22 was used, for the Title III monitoring that was used,
10:17:18AM 23 disclosing to those courts the necessity for this
10:17:22AM 24 technique, the fact that this site had to continue to
10:17:24AM 25 operate in order to give law enforcement an opportunity to

10:17:27AM 1 identify the perpetrators. It was a brief continued
10:17:32AM 2 operation, again, an enterprise that had existed for six
10:17:36AM 3 months, rather than shut it down the date of seizure, 14
10:17:39AM 4 more days, and that's all, in an effort to use
10:17:42AM 5 court-authorized techniques to monitor users in the hope
10:17:46AM 6 of identifying them.

10:17:47AM 7 Now, it is certainly the case, your Honor, that law
10:17:56AM 8 enforcement could have made the decision of shuttering the
10:17:58AM 9 website on the date that it was seized. In many other
10:18:01AM 10 contexts of investigation that is also the case. In
10:18:04AM 11 long-term fraud investigations, in long-term narcotics
10:18:08AM 12 investigations, there are innumerable points in which law
10:18:13AM 13 enforcement can decide to take an action which would
10:18:16AM 14 shutter the organization. This is not the only context in
10:18:19AM 15 which law enforcement faces those sorts of choices.

10:18:25AM 16 So here, the shutting down that website undoubtedly
10:18:29AM 17 would have stopped criminals from being able to use that
10:18:32AM 18 website in order to traffic child pornography images and
10:18:37AM 19 videos on Tor. It would have taken away that one
10:18:40AM 20 particular facility. But it certainly would not and did
10:18:43AM 21 not put an end to the users' ability to continue
10:18:48AM 22 committing those crimes, to the users' ability to continue
10:18:51AM 23 to abuse children, produce images, and then share them
10:18:55AM 24 with others, and to the users' ability to traffic in those
10:18:59AM 25 images. And that is because without taking action to

10:19:01AM 1 identify the perpetrators, those perpetrators go on and
10:19:06AM 2 continue with their criminal conduct, and as we have
10:19:08AM 3 articulated in our filings, simply create new websites
10:19:13AM 4 that operate the same or similarly.

10:19:15AM 5 As of today, on the Tor network, there are child
10:19:18AM 6 pornography websites that operate similarly to this
10:19:21AM 7 particular site, users who can remain anonymous while
10:19:26AM 8 trafficking in child pornography, and users who remain
10:19:29AM 9 unidentified, criminals who remained unidentified.

10:19:31AM 10 Just shutting down the website is not enough. The
10:19:34AM 11 obligation of law enforcement for the government is to
10:19:37AM 12 take some action to identify the perpetrators, and
10:19:41AM 13 identify the victims, and to get those children away,
10:19:44AM 14 where we can, from those abusers. That's the purpose.
10:19:48AM 15 That's the necessity behind a site like this continuing to
10:19:52AM 16 operate, so that crucial IP address information, which
10:19:58AM 17 ultimately leads to being able to identify a perpetrator,
10:20:02AM 18 being able to use further investigation and legal
10:20:06AM 19 processes, to then take that IP information and translate
10:20:09AM 20 it into identifying a person who is trafficking in child
10:20:12AM 21 pornography, or abusing a child and trafficking in child
10:20:14AM 22 pornography.

10:20:15AM 23 So it is in that context that the court has to view
10:20:20AM 24 the government's actions here. And viewed in that light,
10:20:23AM 25 the necessity of identifying the perpetrators, not just

10:20:28AM 1 taking away one particular place where they can
10:20:31AM 2 perpetrate, but taking action -- where they had the
10:20:33AM 3 opportunity and the court authorization to do so, taking
10:20:38AM 4 that action to take that step to identify the victims,
10:20:45AM 5 justifies the -- again, combined with the court
10:20:48AM 6 authorization here, your Honor, justifies the actions
10:20:49AM 7 taken by law enforcement. These are not -- It is not
10:20:53AM 8 outrageous conduct by law enforcement. This is conduct by
10:20:55AM 9 law enforcement that is necessary to enforce the law.

10:21:00AM 10 In terms of the -- The defense has raised some issues
10:21:03AM 11 about the -- at times, about the legality of the actions
10:21:07AM 12 in terms of law enforcement taking enforcement actions
10:21:12AM 13 that when committed by a private citizen would be
10:21:15AM 14 otherwise illegal.

10:21:16AM 15 That is something that, of course, courts have
10:21:18AM 16 recognized, and have recognized for a long time that that
10:21:21AM 17 occurs, that in the course of enforcing laws, law
10:21:25AM 18 enforcement often commits actions that when committed by a
10:21:28AM 19 private citizen would otherwise be unlawful. But that
10:21:32AM 20 doesn't mean that law enforcement is not permitted to take
10:21:34AM 21 those sorts of actions during the course of enforcing the
10:21:37AM 22 law. And that is the context that we operated in here.

10:21:43AM 23 For the legal principle on that, your Honor, I would
10:21:46AM 24 point the court to United States versus Mack, that is 164
10:21:51AM 25 F.3d 467, particularly Page 472. That is a 1999 Ninth

10:21:59AM 1 Circuit opinion. Mack assessed a situation where local
10:22:03AM 2 law enforcement agencies were found to be able, without
10:22:07AM 3 committing crimes against other -- without committing
10:22:10AM 4 crimes against -- possession of prohibited weapons, that
10:22:15AM 5 in order to enforce the law they were permitted to possess
10:22:19AM 6 those, even where possession would be unlawful if done by
10:22:21AM 7 a private citizen, and then take action to prosecute
10:22:25AM 8 defendants.

10:22:27AM 9 The court recognized the longstanding principle, "The
10:22:31AM 10 law has long recognized the reach of a
10:22:33AM 11 strictly-constructed statute stops short of nonsensical
10:22:37AM 12 consequences. The Supreme Court has recognized that a
10:22:40AM 13 statute shall be construed to exempt the government if
10:22:43AM 14 application of the statute to the government would create
10:22:45AM 15 an absurdity."

10:22:47AM 16 Here, in the context of the investigation of online
10:22:49AM 17 child pornography crimes, it is obviously necessary for
10:22:52AM 18 law enforcement to engage in actions that would -- when
10:22:56AM 19 performed by a private individual, would otherwise be
10:22:59AM 20 illegal.

10:23:00AM 21 For example, in order to review and document a
10:23:02AM 22 website, such as the one in this case, law enforcement has
10:23:05AM 23 to access it in an undercover capacity, and access child
10:23:09AM 24 pornography in an undercover capacity. That would be a
10:23:12AM 25 violation of law if done by a private individual. We

10:23:16AM 1 certainly don't look at that as a violation of the law
10:23:19AM 2 when done by an agent who is investigating a crime, and
10:23:21AM 3 taking that action during the course of the investigation.
10:23:23AM 4 Law enforcement has to document child pornography, receive
10:23:26AM 5 it, download it, possess it. And all of those actions and
10:23:30AM 6 those federal statutes, if done -- all of those actions if
10:23:34AM 7 done by a private individual would be a violation of law.
10:23:37AM 8 But that is not the case where done under color of law by
10:23:40AM 9 a law enforcement agent during the course of an
10:23:43AM 10 investigation in order to investigate and to identify
10:23:48AM 11 particular criminals. I did want to make that point, your
10:23:53AM 12 Honor.

10:23:54AM 13 On the necessity principle, and the defense has sort
10:24:00AM 14 of alluded to -- without really putting any particular
10:24:03AM 15 facts in the record, alluded to other actions short of
10:24:07AM 16 running the website that law enforcement could have taken.

10:24:10AM 17 And there is a common-sense principle here regarding
10:24:13AM 18 that, your Honor. And so the defense suggests, you know,
10:24:16AM 19 if the government had just made all of the child
10:24:19AM 20 pornography on the website inaccessible, it could have
10:24:22AM 21 then gone on with the enforcement there. Well, a common
10:24:25AM 22 sense principle, your Honor, says where users for months
10:24:29AM 23 upon months have been able to freely access and distribute
10:24:33AM 24 child pornography through the site, and then one day that
10:24:35AM 25 site has all of a sudden completely different

10:24:38AM 1 functionality and no longer presents any ability to access
10:24:41AM 2 those sorts of materials, well, that would be a tip-off,
10:24:44AM 3 and a tip-off to law enforcement infiltration. And so I
10:24:49AM 4 don't believe it is a reasonable -- Just from a
10:24:51AM 5 common-sense principle, it is certainly understandable
10:24:53AM 6 that the functionality of a site like this would need to
10:24:56AM 7 remain intact in order to give law enforcement the
10:25:00AM 8 opportunity to identify the perpetrators, who would be
10:25:02AM 9 likely scared away or would stop using the facility if it
10:25:07AM 10 turned into something that it wasn't before.

10:25:11AM 11 That's the heart of the reason why it needed to remain
10:25:14AM 12 operating in a similar manner, and in the manner in which
10:25:19AM 13 it had been operating for months and months and months, in
10:25:23AM 14 order to give law enforcement the opportunity to take the
10:25:25AM 15 court-authorized actions to actually identify the
10:25:28AM 16 end-users who were involved in the crimes that were being
10:25:32AM 17 investigated.

10:25:33AM 18 Just a couple of points in terms of specific arguments
10:25:40AM 19 by the defendant. There was a statement that the defense
10:25:48AM 20 was not -- was not aware, or might not have been aware,
10:25:51AM 21 that law enforcement in prior cases has in fact taken
10:25:54AM 22 these sorts of actions on websites -- on child pornography
10:25:58AM 23 websites and on the Tor network. And it is correct -- it
10:26:01AM 24 is in fact a matter of public record that law enforcement
10:26:04AM 25 has in the past seized child pornography websites, allowed

10:26:08AM 1 them to continue to operate in a government facility,
10:26:12AM 2 gotten court authority to deploy a network investigative
10:26:16AM 3 technique, and gotten court authority to conduct Title III
10:26:20AM 4 monitoring.

10:26:21AM 5 The defense has been aware of this for some time. I
10:26:23AM 6 am not sure of the source of the confusion. But the
10:26:25AM 7 defense actually attached a warrant authorizing just that
10:26:28AM 8 from the Nebraska case that both parties have cited a
10:26:32AM 9 number of times. And that warrant authorized a network
10:26:35AM 10 investigative technique involving a website takeover,
10:26:38AM 11 disclosed to the court that law enforcement was going to
10:26:41AM 12 operate that site in order to conduct the monitoring and
10:26:44AM 13 deploy the NIT. I am not sure where the confusion comes
10:26:47AM 14 from.

10:26:49AM 15 But it is certainly the case that law enforcement has
10:26:52AM 16 taken actions like this in the past. And, again, done it
10:26:55AM 17 with court approval. Court approval to deploy the
10:26:59AM 18 investigative technique, court approval to conduct T III
10:27:02AM 19 monitoring to monitor users' communications.

10:27:06AM 20 And those cases -- the Omaha cases have been publicly
10:27:11AM 21 reported. There have been trials that are held in public
10:27:13AM 22 regarding those investigations and a number of individuals
10:27:17AM 23 convicted in the District of Nebraska regarding those
10:27:20AM 24 cases. Again, a matter of public record. And one that
10:27:25AM 25 the defense has cited to a number of times through the

10:27:28AM 1 course of our various pleadings in this case.

10:27:30AM 2 As to the interplay of probable cause to the motion to
10:27:48AM 3 dismiss, your Honor, I am not sure exactly how that really
10:27:53AM 4 comes into play, other than to say that certainly the
10:27:57AM 5 magistrate who issued the NIT warrant found probable
10:28:02AM 6 cause. The district judge who issued the wiretap warrant
10:28:05AM 7 found cause to issue that and to allow that technique.

10:28:11AM 8 And I can tell your Honor, and I have disclosed this
10:28:14AM 9 to the defense, there is and will be issued, I believe
10:28:17AM 10 today, in the Eastern District of Wisconsin, a report and
10:28:21AM 11 recommendation by a magistrate judge regarding a motion to
10:28:24AM 12 suppress involving the NIT warrant in this case, in which
10:28:28AM 13 that magistrate judge, reviewing a probable cause
10:28:31AM 14 challenge to this NIT warrant, found that the warrant
10:28:34AM 15 sufficiently established probable cause. We will provide
10:28:38AM 16 a copy to counsel and to the court as soon as that becomes
10:28:40AM 17 available on the docket.

10:28:43AM 18 But that court reviewing this same NIT warrant came to
10:28:46AM 19 the conclusion that it did articulate probable cause to
10:28:49AM 20 deploy the technique, sufficiently established probable
10:28:53AM 21 cause. It also found, with respect to a Rule 41 argument,
10:28:57AM 22 that suppression was unwarranted in the case based on the
10:29:01AM 23 government's conduct, which it found to be reasonable. We
10:29:04AM 24 will present that to the court, again, once it is
10:29:07AM 25 available.

10:29:07AM 1 To the extent we are talking about probable cause and
10:29:11AM 2 findings of probable cause based on what is articulated in
10:29:14AM 3 the NIT warrant here, that is such a finding by another
10:29:16AM 4 magistrate, in addition to, of course, the issuing
10:29:19AM 5 magistrate who found so here.

10:29:24AM 6 So I gather, your Honor, just in terms of the rest of
10:29:35AM 7 the argument, we will be addressing the particular
10:29:39AM 8 suppression issues separately --

10:29:41AM 9 THE COURT: It is a different issue.

10:29:43AM 10 MR. BECKER: Very well. If I could have the
10:29:52AM 11 court's indulgence to just consult briefly with colleagues
10:29:55AM 12 before I conclude?

10:29:56AM 13 THE COURT: You know, I asked in my order setting
10:30:00AM 14 this hearing up for brief argument on the motion to
10:30:03AM 15 dismiss. I haven't heard anything brief from either side
10:30:06AM 16 on this motion yet.

10:30:11AM 17 MR. BECKER: Very well. I will conclude, your
10:30:13AM 18 Honor.

10:30:13AM 19 THE COURT: I have heard what you have said. You
10:30:16AM 20 guys have to bear in mind I read your briefs, you know. I
10:30:20AM 21 have read them twice. You don't have to repeat what's in
10:30:24AM 22 your briefs.

10:30:24AM 23 Mr. Fieman, do you have any response?

10:30:27AM 24 MR. FIEMAN: Not without repeating myself, your
10:30:30AM 25 Honor. One brief point. Two brief points. One is this,

10:30:34AM 1 your Honor: You can search in vain every one of those
10:30:38AM 2 Nebraska warrants, the NIT warrant, any of the warrants,
10:30:41AM 3 and you will not find a single reference to the government
10:30:44AM 4 continuing to distribute pornography as part of their
10:30:47AM 5 investigation.

10:30:48AM 6 It has been routine -- And we do not dispute that the
10:30:51AM 7 government can take over websites and collect identifying
10:30:54AM 8 data in that process. In fact, that's what they asked
10:30:57AM 9 Judge Buchanan to do, to collect the IP address at log-in.
10:31:03AM 10 Nowhere in any of these cases have they disclosed in their
10:31:06AM 11 warrants that they intended to continue to actively
10:31:08AM 12 distribute child pornography. That is a revelation, and
10:31:11AM 13 it is appalling, because there is in fact no investigatory
10:31:14AM 14 need. It is a false choice between shuttering down this
10:31:18AM 15 site and the extra step of allowing people to post and
10:31:22AM 16 distribute.

10:31:23AM 17 The other very brief thing I would say, your Honor,
10:31:29AM 18 that really goes to the crux of both the PC and outrageous
10:31:34AM 19 conduct, because if the government is alleging that they
10:31:37AM 20 have probable cause to collect the IP address at log-in,
10:31:41AM 21 they have accomplished their investigatory goal. Now it
10:31:45AM 22 is a separate issue whether PC is in fact established, and
10:31:48AM 23 we will further address that during the course of the
10:31:50AM 24 later arguments, your Honor.

10:31:52AM 25 THE COURT: This is a motion to dismiss based on

1 outrageous government conduct, as moved in Docket 50 by
2 the defense. This does not require an analysis of whether
3 the government did the right thing or whether the
4 government made errors, or whether the showing was
5 sufficient on the warrants, or whether evidence collected
6 on the basis of the warrant should be suppressed. It is a
7 question of whether the government's conduct in this whole
8 process is so grossly shocking and so outrageous as to
9 violate the universal sense of justice, and offend canons
10 of decency and fairness, violate notions of justice. This
11 motion has not reached that standard that the defense
12 would have to show.

13 I just have a couple of comments about it. First, the
14 government did, from what I have read here, seize and
15 control a website that contained child pornography, and
16 kept it alive. Arguably that was under the government's
17 control, as the statute requires that they handle evidence
18 of child pornography. I mean, you can argue about that,
19 but it is arguable, and a reasonable position to take,
20 that they controlled that site consistent with that
21 statute.

22 We will investigate further today the motion to
23 suppress. But in the government's seeking of warrants and
24 seizing of evidence, the evidence shows that they were
25 trying to catch the bad guys, so to speak, that they were

10:34:30AM 1 doing their work as law enforcement agents. Whether they
10:34:34AM 2 did it right is a different thing. But they didn't do it
10:34:38AM 3 so wrong as to be grossly shocking or outrageous to
10:34:44AM 4 violate the universal sense of justice.

10:34:48AM 5 It is easy to argue, and, my gosh, we hear it in all
10:34:54AM 6 kinds of cases, that the other side's position is
10:34:57AM 7 outrageous. Well, you know, that's a high standard. From
10:35:08AM 8 the standpoint of one who stands between the defendant and
10:35:11AM 9 the government, and represents neither side, you look at
10:35:18AM 10 what happened and look inward. I am not shocked by this.
10:35:26AM 11 I did not find it outrageous.

10:35:32AM 12 Whether there are grounds to suppress evidence here is
10:35:35AM 13 an entirely different issue, but there is no basis to
10:35:43AM 14 dismiss the indictment based on outrageous conduct. That
10:35:46AM 15 motion made in Docket 50 is denied.

10:35:57AM 16 I guess the next issue to address is the evidentiary
10:36:13AM 17 hearing, if necessary, and argument on the motions to
10:36:17AM 18 suppress. Those motions are made in three separate
10:36:23AM 19 documents, Dockets 26, 50, and 65.

10:36:36AM 20 The government has the burden of going forward on this
10:36:39AM 21 issue. I guess I would like to know what you anticipate
10:36:44AM 22 showing, and would ask you for a brief, brief, like five
10:36:52AM 23 minutes, opening statement. You can bear in mind that I
10:37:04AM 24 am mindful of the issues that I anticipate you will be
10:37:08AM 25 generally addressing. I am more curious as to how you

10:37:12AM 1 propose to proceed and what you propose to show.

10:37:15AM 2 MR. BECKER: Understood, your Honor. It appears
10:37:18AM 3 that we are in a scenario where the court has denied the
10:37:21AM 4 request for a Franks hearing, and the defense, I believe,
10:37:24AM 5 is taking the position that the issues related to
10:37:28AM 6 suppression can be decided based upon the paper record.
10:37:32AM 7 So I think that would be our intent in proceeding.

10:37:35AM 8 Now, this is a bit of a shift in the footing. We
10:37:39AM 9 certainly are available to present testimony, but at this
10:37:44AM 10 point I think we would intend to proceed on the paper
10:37:47AM 11 record. There are exhibits that I think both parties will
10:37:51AM 12 agree can be entered as a part of the proceeding
10:37:54AM 13 pertaining to warrant documents and the like, and perhaps
10:38:00AM 14 some others that I think we agreed on that can be put into
10:38:05AM 15 the record.

10:38:06AM 16 THE COURT: I have some questions for somebody,
10:38:08AM 17 maybe counsel can answer them, about how this worked. I
10:38:14AM 18 am not asking for an evidentiary showing. I just want you
10:38:18AM 19 to have the opportunity to make whatever showing you feel
10:38:20AM 20 is necessary.

10:38:25AM 21 MR. BECKER: In terms of the suppression issues, I
10:38:29AM 22 think we intend to stand on the paper record and argue
10:38:34AM 23 from the documents.

10:38:37AM 24 THE COURT: Okay.

10:38:39AM 25 MR. FIEMAN: Unless there are questions that I

10:38:41AM 1 can't answer and our expert can, your Honor, I would ask
10:38:45AM 2 the court to proceed on the paper record. I will alert
10:38:48AM 3 the court if there is something beyond that scope.

10:38:52AM 4 THE COURT: Let me ask these questions preliminary
10:38:55AM 5 to anything else. Not the questions that I raised in my
10:39:05AM 6 order setting up this hearing. When the government got
10:39:24AM 7 the authority to attach this NIT to the website, how do
10:39:34AM 8 you do that? Does somebody sit down on a computer and
10:39:38AM 9 make keystrokes to make that happen? How is that done?

10:39:43AM 10 MR. FIEMAN: Your Honor, I can tell you, based on
10:39:45AM 11 that question alone, we will need testimony from
10:39:50AM 12 Mr. Soghoian on the part of the defense. He is quite
10:39:52AM 13 capable of saying this in layman terms, but I do not want
10:39:56AM 14 him to state the process.

10:39:58AM 15 THE COURT: Anyway, I am curious about that. And
10:40:04AM 16 then once it is attached to the website, and it goes
10:40:16AM 17 out -- as I understand it, then it goes out to users of
10:40:23AM 18 the website who have to sign in. When they sign in, does
10:40:26AM 19 it pick up whatever information it is going to pick up
10:40:29AM 20 automatically, or when they enter into that website are
10:40:40AM 21 they directed to enter some other information by this NIT,
10:40:49AM 22 or does it happen automatically without any additional
10:40:55AM 23 entries?

10:40:57AM 24 MR. FIEMAN: I can give you a brief response to
10:40:59AM 25 all three, your Honor. The first question is how is the

10:41:14AM 1 NIT programmed. That is part of what we don't know. But
10:41:16AM 2 typically in NIT cases, what it is is a set of code
10:41:20AM 3 components that work in conjunction to do really a very
10:41:23AM 4 simple thing. When a user signs -- is signed into the
10:41:30AM 5 homepage, that activity triggers -- either automatically
10:41:34AM 6 or by an agent monitoring the log-in, we do not know yet,
10:41:39AM 7 but, regardless, at the point of sign-in this code is sent
10:41:45AM 8 from the Virginia server to the target computer, in this
10:41:50AM 9 case allegedly Mr. Michaud's. And that is what it is, it
10:41:54AM 10 is code, it is data.

10:41:57AM 11 That code breaks through any security barriers that
10:42:01AM 12 might impede it --

10:42:01AM 13 THE COURT: You know, I know that. What does
10:42:05AM 14 Mr. Michaud do?

10:42:07AM 15 MR. FIEMAN: What he is alleged to have done is
10:42:10AM 16 signed into the website.

10:42:11AM 17 THE COURT: As always, or per usual, or does he
10:42:14AM 18 have to enter in some other information?

10:42:17AM 19 MR. FIEMAN: No.

10:42:18AM 20 THE COURT: Does it tell him, to get in, you have
10:42:20AM 21 to do one, two, three?

10:42:22AM 22 MR. FIEMAN: The homepage has like a user name, as
10:42:25AM 23 you log into anything, like email. So there are about a
10:42:29AM 24 hundred thousand people who are logging in. At the moment
10:42:32AM 25 they are typing in their log-in at that homepage, the NIT

10:42:36AM 1 is sent to the target computer and begins extracting data
10:42:40AM 2 here in Washington.

10:42:41AM 3 THE COURT: Without any additional action on the
10:42:45AM 4 part of the user?

10:42:46AM 5 MR. FIEMAN: None whatsoever. Did I address your
10:42:57AM 6 questions so far?

10:42:59AM 7 THE COURT: Yes. Do the FBI experts have any way
10:43:14AM 8 to look at the NIT information other than going to the
10:43:24AM 9 server?

10:43:28AM 10 MR. FIEMAN: Your Honor, they don't go to the
10:43:29AM 11 server.

10:43:30AM 12 THE COURT: Where do they go? How do they get the
10:43:33AM 13 information?

10:43:35AM 14 MR. FIEMAN: They get it from Mr. Michaud's
10:43:38AM 15 computer.

10:43:38AM 16 THE COURT: They don't have his computer.

10:43:41AM 17 MR. FIEMAN: That's what the NIT is for.

10:43:43AM 18 THE COURT: His information -- You see, this is
10:43:45AM 19 what is confusing to me. It has a lot to do with where
10:43:50AM 20 the search occurred. How do they find information? Maybe
10:44:00AM 21 you need to call a witness on these things.

10:44:03AM 22 MR. BECKER: Our lawyer argument is one thing, in
10:44:08AM 23 terms of explaining the network investigative technique.
10:44:13AM 24 I do think we need to be clear on the record the footing
10:44:16AM 25 and how, if at all, these questions play into the court

1 authorization and the particular -- any particular
2 challenges to it, so that, I guess, we know -- actually,
3 the government knows what footing we are on so we can
4 elect to present testimony and what that is pertinent to.

5 Certainly the warrant itself and the affidavit does
6 give an explanation of how the NIT will work and operate.

7 THE COURT: It doesn't explain the things I am
8 asking about.

9 MR. BECKER: Some of them are addressed, your
10 Honor. If I could just have -- Your Honor, I would point
11 to Paragraph 33 on Page 24 of the NIT warrant.

12 THE COURT: That is the Rule 41 application?

13 MR. BECKER: Correct. This is Exhibit 1 to
14 Government Docket No. 47.

15 THE COURT: Page and line again.

16 MR. BECKER: Page 24, Paragraph 33.

17 THE COURT: 24 at the top, the docket pages, or 24
18 at the bottom?

19 MR. BECKER: Sorry. 24 at the bottom, your Honor.

20 THE COURT: Paragraph 33.

21 MR. BECKER: Yes, your Honor. And that does give
22 a description of how the process of the NIT operates. And
23 that is, "In the normal course of operation websites sent
24 content to visitors."

25 THE COURT: Just a minute. Let me read it.

10:46:32AM 1 MR. BECKER: Yes, your Honor.

10:47:01AM 2 THE COURT: You see, that is the kind of paragraph
10:47:03AM 3 I don't understand fully. And I am trying to understand.
10:47:13AM 4 Under the NIT authorization the website would augment that
10:47:20AM 5 content with additional computer instructions. When a
10:47:27AM 6 user's computer successfully downloads those instructions
10:47:33AM 7 it causes the computer -- the activating computer to
10:47:41AM 8 transmit certain information. That sounds like the user
10:47:43AM 9 has to download some instructions in addition to just
10:47:47AM 10 signing into the website.

10:47:50AM 11 MR. BECKER: The warrant specifically authorized
10:47:52AM 12 the government to deploy the NIT to any user who did log
10:47:59AM 13 into the website with a user name and a password. And so
10:48:02AM 14 the authorization permitted the government to deploy the
10:48:06AM 15 NIT to any user who went that far.

10:48:07AM 16 THE COURT: I know that. I am trying to find out
10:48:09AM 17 how this works.

10:48:11AM 18 MR. BECKER: Understood.

10:48:12AM 19 THE COURT: So what does the user do? Are there
10:48:16AM 20 new instructions when he signs into the website?

10:48:20AM 21 MR. BECKER: Yes, your Honor. That's what the
10:48:25AM 22 word "augment" references, is that in addition to the
10:48:28AM 23 instructions --

10:48:28AM 24 THE COURT: What do the instructions say?

10:48:31AM 25 MR. BECKER: The use of the word "augment" means

10:48:37AM 1 that these are additional instructions beyond the normal
10:48:40AM 2 instructions that would be on the website. We do think --
10:48:45AM 3 That is articulated.

10:48:47AM 4 The specific instructions -- what the instructions
10:48:50AM 5 are, what the code is, is not articulated in the warrant,
10:48:53AM 6 that is correct. The computer code is not. What is
10:48:56AM 7 articulated in the warrant is that there are computer
10:48:59AM 8 instructions that are sent to the user's computer, the
10:49:03AM 9 activating computer, and that causes, as articulated in
10:49:06AM 10 the warrant, the activating computer to send the specified
10:49:09AM 11 information --

10:49:11AM 12 THE COURT: Let's talk about what the user does.
10:49:13AM 13 He signs into the website?

10:49:16AM 14 MR. BECKER: Yes.

10:49:18AM 15 THE COURT: Now, does the website send him these
10:49:21AM 16 instructions that he has to enter more things in
10:49:26AM 17 compliance with those instructions? I am talking to the
10:49:30AM 18 wrong guys here.

10:49:32AM 19 MR. FIEMAN: I can't answer this question, your
10:49:34AM 20 Honor. It is just that I don't think Mr. Becker wants to.

10:49:37AM 21 MR. BECKER: Your Honor, at this point I want to
10:49:41AM 22 make argument from the warrant itself. I do think that is
10:49:44AM 23 important. And I do believe --

10:49:45AM 24 THE COURT: We are not to argument from the
10:49:47AM 25 warrant yet. We are still at the point of trying to find

10:49:50AM 1 out what happened. I want to know what happened, how it
10:49:56AM 2 works.

10:50:04AM 3 MR. BECKER: Can I have a quick moment to confer
10:50:09AM 4 with counsel?

10:50:09AM 5 THE COURT: It is time we took a break anyway. I
10:50:11AM 6 want to know what the user has to do to trigger this NIT,
10:50:19AM 7 if anything. Then I want to know what does the FBI guy do
10:50:28AM 8 to find out where -- the information that the NIT
10:50:34AM 9 provides, how does he get that? I suppose there is
10:50:37AM 10 somebody sitting in a cubicle somewhere with a keyboard
10:50:42AM 11 doing this stuff. I don't know that. It may be they seed
10:50:51AM 12 the clouds, and the clouds rain information. I don't
10:50:55AM 13 know.

10:50:56AM 14 MR. BECKER: Understood, your Honor. While we are
10:50:58AM 15 breaking, are there other questions that your Honor has?
10:51:03AM 16 I can confer --

10:51:03AM 17 THE COURT: Those are the main ones. There may be
10:51:06AM 18 others that come to mind as we argue this matter.

10:51:09AM 19 MR. BECKER: Thank you, your Honor.

10:51:15AM 20 THE COURT: We will reconvene shortly after 11:00.

11:10:21AM 21 (Break.)

11:10:21AM 22 THE COURT: My staff says they think these
11:10:23AM 23 instructions are computers talking to each other, and that
11:10:28AM 24 the information is sent from the user's computer back
11:10:38AM 25 without the user making any additional computer

11:10:41AM 1 keystrokes. Right?

11:10:44AM 2 MR. BECKER: That's correct, your Honor.

11:10:46AM 3 THE COURT: Do you agree?

11:10:47AM 4 MR. FIEMAN: Yes, your Honor.

11:10:51AM 5 THE COURT: My next question then is, what happens
11:10:56AM 6 when Mr. FBI Agent wants to see if anybody signed in? So
11:11:07AM 7 they put the NIT on here, he goes home for the night, some
11:11:12AM 8 FBI agents sleep, but not much, and he comes in in the
11:11:18AM 9 morning. What does he do to see if there is any
11:11:23AM 10 information on there?

11:11:23AM 11 MR. BECKER: Let me first articulate, your Honor,
11:11:26AM 12 as we have articulated in our filing in response to the
11:11:29AM 13 motion to compel, the site was monitored 24 hours a day,
11:11:34AM 14 seven days a week, while it was in FBI control. There was
11:11:36AM 15 not a point where this site was being operated --
11:11:40AM 16 administered by the FBI that it was not being monitored by
11:11:44AM 17 the FBI.

11:11:45AM 18 THE COURT: You mean they don't even get up and go
11:11:47AM 19 to the restroom? Regardless, what happens on the FBI end?

11:12:00AM 20 MR. BECKER: The information that is returned by
11:12:02AM 21 the NIT is delivered to an FBI computer.

11:12:05AM 22 THE COURT: And how does the FBI agent get that
11:12:08AM 23 information?

11:12:09AM 24 MR. BECKER: That information is loaded into a
11:12:12AM 25 system that turns it into a report, and then those reports

11:12:16AM 1 are generated. That report -- Actually, I can proffer
11:12:20AM 2 into evidence Exhibit 15. That report contains for a
11:12:26AM 3 particular user all of the actions that the user took on
11:12:29AM 4 the website.

11:12:30AM 5 THE COURT: How does the FBI agent get that
11:12:33AM 6 information?

11:12:36AM 7 MR. BECKER: From the FBI computer on which it is
11:12:38AM 8 stored.

11:12:38AM 9 THE COURT: So he has to sit at his computer and
11:12:41AM 10 make some keystrokes for this to come up, or open his
11:12:47AM 11 computer, or something?

11:12:52AM 12 MR. BECKER: In order to access the data that is
11:12:55AM 13 stored on the computer, yes, you would have to go on to
11:12:58AM 14 that computer and see, okay, what information was
11:13:00AM 15 returned. And that is generated into reports that we have
11:13:03AM 16 provided.

11:13:03AM 17 THE COURT: Where is that information that he or
11:13:08AM 18 she is now looking?

11:13:17AM 19 MR. BECKER: At the time the data is returned it
11:13:19AM 20 is on the government's computer in Virginia, the computer
11:13:22AM 21 to which that information is returned.

11:13:24AM 22 THE COURT: Does he have any ability to go back to
11:13:29AM 23 the user's computer and look in there, see what else he
11:13:33AM 24 can find?

11:13:39AM 25 MR. BECKER: No, your Honor. We can put on

11:13:44AM 1 testimony regarding these questions. As the warrant makes
11:13:52AM 2 clear, this was not something that sat on the user's
11:13:55AM 3 computer. Let me -- We can put on testimony to clarify
11:13:59AM 4 some of these questions, your Honor. I think that is
11:14:01AM 5 probably the best way forward.

11:14:02AM 6 THE COURT: If you want to, I would like to know
11:14:05AM 7 how this works.

11:14:06AM 8 MR. BECKER: Indeed. Understood, your Honor.
11:14:09AM 9 Just for the court's benefit, and I don't mean for us to
11:14:12AM 10 be obstreperous at all, there may be questions or areas
11:14:16AM 11 where if it involves a level of detail about information
11:14:20AM 12 pertaining to the network --

11:14:22AM 13 THE COURT: I don't want the detail. It wouldn't
11:14:24AM 14 mean anything to me anyway. But I understand enough to
11:14:30AM 15 know that if you want to see something on your computer,
11:14:34AM 16 you have to turn it on and hit the right strokes, or else
11:14:39AM 17 you are just in there playing solitaire or something. I
11:14:46AM 18 don't care what the strokes are. I don't care about that.
11:14:51AM 19 I just want to know what's available and how they would do
11:14:55AM 20 it.

11:14:55AM 21 MR. BECKER: At this time we would call Special
11:15:00AM 22 Agent Dan Alfin to the stand.

23 DANIEL ALFIN

11:15:40AM 24 Having been sworn under oath, testified as follows:

11:15:40AM 25 DIRECT EXAMINATION

11:15:42AM 1 By Mr. Becker:

11:15:43AM 2 Q. Please state and spell your full name for the record.

11:15:45AM 3 A. My name is Daniel Alfin, D-A-N-I-E-L, A-L-F-I-N.

11:15:54AM 4 Q. What do you do for a living?

11:15:55AM 5 A. I am a special agent with the FBI. I am currently
11:15:59AM 6 assigned to FBI headquarters, criminal investigative
11:16:04AM 7 division, violent crimes against children section, major
11:16:07AM 8 case coordination unit, located in Linthicum, Maryland.

11:16:12AM 9 Q. And how long have you been with the FBI?

11:16:15AM 10 A. I have been employed with the FBI for approximately
11:16:18AM 11 six years.

11:16:18AM 12 Q. What are the responsibilities of your unit, the major
11:16:24AM 13 case coordination unit?

11:16:26AM 14 A. The major case coordination unit conducts large-scale
11:16:30AM 15 investigations of online child exploitation offenders that
11:16:34AM 16 typically have a nationwide or international nexus.

11:16:37AM 17 Q. For how long have you been in that particular unit of
11:16:41AM 18 the FBI?

11:16:42AM 19 A. I have been assigned to the major case coordination
11:16:45AM 20 unit since approximately July 2014.

11:16:49AM 21 Q. What sorts of roles and responsibilities do you have
11:16:52AM 22 within that unit?

11:16:53AM 23 A. In my role as a special agent at the major case
11:16:57AM 24 coordination unit I routinely conduct investigations of
11:17:01AM 25 offenders who utilize sophisticated technology to

1 obfuscate or cover up their child exploitation activities.
2 A significant amount of my time at the major case
3 coordination unit has been dedicated to investigating
4 child sex offenders who utilize the Tor network to engage
5 in the advertisement, distribution, and production of
6 child pornography.

7 Q. Have you accessed websites -- child pornography
8 websites on the Tor network in an undercover capacity?

9 A. I have. I have accessed, documented, and reviewed
10 numerous websites that exist and have existed on the Tor
11 network, whose primary purposes were the advertisement and
12 distribution of child pornography.

13 Q. Special Agent Alfin, did you participate in the
14 investigation of the website that is pertinent to this
15 case, that we have referred to as Website A?

16 A. I did.

17 Q. Can you just go back and just describe -- How did
18 you become aware of Website A, initially?

19 A. I became aware of Website A approximately August 2014
20 when it came online. At that point in time links to
21 Website A were advertised on multiple websites, whose
22 purposes were the advertisement of websites dedicated to
23 the advertisement and distribution of child pornography.

24 After I saw the link to Website A come online, I
25 accessed it and observed that it was in fact a website

11:18:37AM 1 whose primary purpose was the advertisement and
11:18:40AM 2 distribution of child pornography. I reviewed the website
11:18:42AM 3 on multiple occasions between August 2014 and March 2015.

11:19:11AM 4 MR. BECKER: Your Honor, I believe the court has
11:19:13AM 5 an evidence binder available. There are a couple of
11:19:16AM 6 exhibits that we will present. I want to make sure the
11:19:18AM 7 court has that in front of him.

11:19:28AM 8 By Mr. Becker:

11:19:28AM 9 Q. Special Agent Alfin, I would direct your attention to
11:19:31AM 10 Exhibit 12A. Do you have the book in front of you?

11:19:35AM 11 A. I do.

11:19:36AM 12 Q. What does Exhibit 12A depict?

11:19:50AM 13 A. In early February 2015 an FBI agent at the major case
11:19:55AM 14 coordination unit accessed Website A in an undercover
11:20:00AM 15 capacity. That agent took multiple screen captures of
11:20:03AM 16 Website A as it appeared during that time. This is one of
11:20:07AM 17 those screen captures. And it depicts the front page of
11:20:10AM 18 Website A prior to logging into the website.

11:20:16AM 19 MR. BECKER: Your Honor, with the court's
11:20:17AM 20 indulgence -- Well, first, I would move to admit
11:20:20AM 21 Exhibit 12A, and then to publish via the computer a copy
11:20:24AM 22 of that exhibit.

11:20:26AM 23 MR. FIEMAN: No objection, your Honor.

11:20:27AM 24 THE COURT: All right. It may be admitted.

11:20:41AM 25 (Exhibit No. 12A was admitted.)

11:20:41AM 1 By Mr. Becker:

11:20:42AM 2 Q. Special Agent Alfin, can you see 12A on your screen?

11:20:50AM 3 A. I can.

11:20:50AM 4 Q. How would the user go about logging into the website?

11:20:54AM 5 A. A user who wanted to log into Website A would have to
11:20:59AM 6 either log into Website A with a previously established
11:21:04AM 7 user name and password, or they would have to click on the
11:21:09AM 8 words that say "register an account." At that point they
11:21:14AM 9 would be taken to the registration screen, where they
11:21:17AM 10 would have to create a user name and password in order to
11:21:20AM 11 log into the website.

11:21:21AM 12 Q. If you can turn in your book to Exhibit 12B?

11:21:38AM 13 A. I have the exhibit in front of me.

11:21:40AM 14 Q. What is Exhibit 12B?

11:21:41AM 15 A. Exhibit 12B shows the index that a user would be
11:21:47AM 16 directed to after logging into Website A with a user name
11:21:52AM 17 and password. The index displays all of the forums
11:21:56AM 18 available within Website A for users to access and
11:22:01AM 19 distribute content.

11:22:04AM 20 MR. BECKER: Your Honor, I move to admit 12B and
11:22:07AM 21 to publish.

11:22:08AM 22 MR. FIEMAN: No objection.

11:22:09AM 23 THE COURT: It may be admitted.

11:22:10AM 24 (Exhibit No. 12B was admitted.)

11:22:10AM 25 By Mr. Becker:

11:22:24AM 1 Q. Special Agent Alfin, on Exhibit 12B, there are a
11:22:30AM 2 number of words in purple type. What are those called?

11:22:34AM 3 A. Those are the various forums available on Website A.
11:22:42AM 4 If a user were to click on one of those purple words they
11:22:46AM 5 would be directed to that particular forum on Website A.
11:22:52AM 6 For example, referring to this exhibit, one of the links
11:22:59AM 7 is under the heading "Preteen Photos," and it is titled,
11:23:05AM 8 "Girls HC."

11:23:07AM 9 Q. Scroll down on the digital version. Do you see the
11:23:20AM 10 particular forum you just mentioned, "Girls HC"?

11:23:24AM 11 A. I do.

11:23:25AM 12 Q. Can you point it out on the monitor?

11:23:29AM 13 A. (Indicating.)

11:23:40AM 14 Q. First, the designation "HC," what does that
11:23:45AM 15 reference?

11:23:45AM 16 A. In the context of a website, such as Website A, HC is
11:23:51AM 17 a common abbreviation for hardcore, which refers to
11:23:56AM 18 penetrative sexual activity.

11:24:00AM 19 Q. And what broader set of forums is that "Girls HC"
11:24:10AM 20 within?

11:24:10AM 21 A. That is under the heading of, "Preteen Videos,"
11:24:13AM 22 indicating that these forums purport to advertise and
11:24:17AM 23 distribute images and videos of prepubescent children
11:24:23AM 24 engaged in hardcore sexual activity.

11:24:25AM 25 Q. If a user clicked on the word -- clicked on that word

11:24:35AM 1 "Girls HC" on the website, what would happen?

11:24:37AM 2 A. At that point the user would be directed to the
11:24:44AM 3 Preteen Videos - Girls Hardcore forum, and they would see
11:24:47AM 4 a listing on their screen all of the topics currently
11:24:49AM 5 available in that forum.

11:24:51AM 6 Q. When you say "topics," what does that mean?

11:24:53AM 7 A. An individual topic within the forum would contain
11:24:59AM 8 links to images and videos of a particular set of images
11:25:03AM 9 of child pornography. In addition to being able to access
11:25:07AM 10 one of these posts, after entering the forum a user would
11:25:10AM 11 also have the option to create a new post and share links
11:25:14AM 12 to images and videos of child pornography.

11:25:23AM 13 THE COURT: It seems to me this is all stuff that
11:25:26AM 14 I have read about.

11:25:29AM 15 MR. BECKER: Indeed, your Honor. We were just
11:25:31AM 16 trying to present some background to get to the questions
11:25:35AM 17 that your Honor had, just in terms of how the site
11:25:38AM 18 functioned.

11:25:38AM 19 THE COURT: Move right along, counsel.

11:25:41AM 20 MR. BECKER: Indeed, your Honor.

11:25:42AM 21 By Mr. Becker:

11:25:45AM 22 Q. Special Agent Alfin, were you familiar with the
11:25:48AM 23 general operation of the network investigative technique
11:25:52AM 24 that was deployed on this website between February 20th
11:25:55AM 25 and March 4th?

11:25:56AM 1 A. I am.

11:25:57AM 2 Q. Were reports generated regarding users, including
11:26:04AM 3 their activity, and information that was collected by the
11:26:07AM 4 NIT?

11:26:08AM 5 A. Yes.

11:26:09AM 6 Q. Was such a report mailed for the user Pewter,
11:26:14AM 7 P-E-W-T-E-R?

11:26:20AM 8 A. Yes.

11:26:20AM 9 Q. Your Honor --

11:26:22AM 10 Special Agent Alfin, can you look at Government's
11:26:26AM 11 Exhibit 15?

11:26:27AM 12 MR. BECKER: Your Honor, I think that is a DVD
11:26:30AM 13 disk that might be in your Honor's binder.

11:26:41AM 14 THE COURT: There is a disk here.

11:26:42AM 15 By Mr. Becker:

11:26:42AM 16 Q. Are you familiar with Government's Exhibit 15?

11:26:45AM 17 A. I am. That is a disk that I created that contains a
11:26:48AM 18 copy of the user accounts for the user Pewter.

11:26:55AM 19 Q. If you can turn to Exhibit 15A in your book.

11:27:02AM 20 MR. BECKER: First, I would move to admit
11:27:04AM 21 Exhibit 15.

11:27:11AM 22 MR. FIEMAN: No objection.

11:27:13AM 23 MR. BECKER: We would move to admit that under
11:27:15AM 24 seal, because it does contain contraband child
11:27:19AM 25 pornography. We would move to admit that under seal.

11:27:22AM 1 MR. FIEMAN: No objection, your Honor.

11:27:23AM 2 THE COURT: It may be admitted under seal.

11:27:26AM 3 (Exhibit No. 15 was admitted.)

11:27:27AM 4 By Mr. Becker:

11:27:28AM 5 Q. Special Agent Alfin, do you have 15A in front of you?

11:27:32AM 6 A. I do.

11:27:32AM 7 Q. What is Exhibit 15A?

11:27:34AM 8 A. Exhibit 15A is a screenshot from the user account --
11:27:40AM 9 that is contained from the report of the Pewter user
11:27:44AM 10 account that is contained on Exhibit 15. This particular
11:27:48AM 11 screenshot contains information about the Pewter user
11:27:51AM 12 account, including that it was logged into Website A for
11:27:56AM 13 approximately 99 hours and 37 minutes over the course of
11:28:00AM 14 the Pewter user account's existence.

11:28:05AM 15 Q. Can you turn to Exhibit 15B?

11:28:12AM 16 A. I have it in front of me.

11:28:15AM 17 Q. What is 15B?

11:28:16AM 18 A. 15B is another screenshot from the Pewter user
11:28:22AM 19 report. This screenshot includes the information that was
11:28:25AM 20 generated by the NIT when it was deployed against the
11:28:29AM 21 Pewter user account.

11:28:33AM 22 MR. FIEMAN: Objection, your Honor. That is a
11:28:36AM 23 misstatement of the report. It is not deployed --

11:28:38AM 24 THE COURT: Speak through the mic.

11:28:41AM 25 MR. FIEMAN: The NIT is not deployed against the

11:28:45AM 1 user account. It is deployed against the target computer.
11:28:49AM 2 That is a statement in the record.

11:28:51AM 3 THE COURT: I guess that is a suggestion to you.
11:28:55AM 4 Is that an objection?

11:28:57AM 5 MR. FIEMAN: Yes, your Honor. It misstates the
11:28:59AM 6 facts already in evidence.

11:29:04AM 7 THE COURT: I am not going to judge that right
11:29:06AM 8 now.

11:29:07AM 9 MR. BECKER: It seems like a semantic argument,
11:29:10AM 10 your Honor. I don't think it would weigh on the
11:29:12AM 11 admissibility of the exhibit.

11:29:14AM 12 THE COURT: Go ahead.

11:29:20AM 13 MR. BECKER: Has 15B been admitted, your Honor? I
11:29:23AM 14 would move to admit 15B.

11:29:26AM 15 MR. FIEMAN: No objection, your Honor.

11:29:27AM 16 THE COURT: It may be admitted.

11:29:34AM 17 (Exhibit No. 15B was admitted.)

11:29:34AM 18 MR. BECKER: Permission to publish.

11:29:36AM 19 By Mr. Becker:

11:29:42AM 20 Q. Special Agent Alfin, just going from left to right on
11:29:45AM 21 Exhibit 15B, can you just indicate what information is
11:29:48AM 22 contained here?

11:29:52AM 23 A. This information shows information that was generated
11:29:55AM 24 by the NIT. The first column is the date and time that
11:30:00AM 25 the NIT collected the information. It indicates that the

11:30:03AM 1 information was collected on or about February 28th, 2015.
11:30:09AM 2 The second column, titled "URL," indicates the specific
11:30:15AM 3 page within Website A that the Pewter user account
11:30:20AM 4 accessed when the NIT collected the information from the
11:30:23AM 5 user account. "Site user name" indicates that the site
11:30:30AM 6 user name was Pewter. "IP address" indicates the IP
11:30:36AM 7 address that was utilized by the Pewter user account on
11:30:41AM 8 that specific date and time. "MAC" refers to MAC address.
11:30:48AM 9 A MAC address is a unique identifier on a network card
11:30:53AM 10 that a user can utilize to connect to the internet. This
11:30:58AM 11 unique identifier is the identifier that was in use by the
11:31:02AM 12 user of the Pewter account on the date and time that the
11:31:06AM 13 NIT collected this information. "Host name" refers to the
11:31:11AM 14 Windows computer name that was in use by the user of the
11:31:16AM 15 Pewter user account on this date and time. "Log on name"
11:31:21AM 16 indicates the Windows user name of the computer that was
11:31:27AM 17 actively using the Pewter user account on this date and
11:31:31AM 18 time. The "user name" column is blank. "OS" refers to
11:31:38AM 19 the operating system of the computer that was utilizing
11:31:42AM 20 the Pewter user account on this date and time.

11:31:48AM 21 Q. And then the column, "IP geo location," was that a
11:31:52AM 22 function of the NIT, or something else?

11:31:53AM 23 A. It was not. The IP geo location fields were
11:32:00AM 24 generated afterwards, not as a function of the NIT.

11:32:05AM 25 Utilizing the IP address that was identified by the NIT,

1 publicly available databases were searched to indicate
2 that IP address on that given date and time was assigned
3 to a Comcast internet -- excuse me, Comcast cable account,
4 located approximately in the area of Vancouver,
5 Washington.

6 Q. Special Agent Alfin, what does this record indicate
7 was the action that triggered the deployment of the NIT to
8 this user?

9 A. In the case of the Pewter user account, this
10 information indicates that an individual logged into
11 Website A with a user name and password, and then
12 navigated to a section of the website that I previously
13 pointed out, entitled, "Preteen Videos - Girls Hardcore,"
14 again, an abbreviation for hardcore. The user accessed
15 this forum, and then they opened a specific post within
16 that forum that purported to advertise images and videos
17 of child pornography. After accessing that particular
18 page on Website A, the NIT collected the information
19 associated with the Pewter user account.

20 Q. And in order to access that particular page, what
21 action would the user take? What would the user
22 physically do?

23 A. The user would have clicked on the title of that
24 post, which was a post indicative of advertising child
25 pornography. After clicking on that post, the NIT would

11:33:45AM 1 have collected the information without anything being
11:33:49AM 2 apparent to the user. The user did not have to take any
11:33:52AM 3 additional actions. Nothing appeared on their screen.
11:33:57AM 4 There was no pop-up message. The activity occurred in the
11:34:01AM 5 background.

11:34:03AM 6 Q. Can you pull up Exhibit 13B?

11:34:12AM 7 A. That exhibit is not in my binder.

11:34:38AM 8 MR. BECKER: Your Honor, Exhibit 13B, because it
11:34:43AM 9 contains contraband images is only in your Honor's binder.

11:34:47AM 10 THE COURT: I didn't hear all of that.

11:34:49AM 11 MR. BECKER: Exhibit 13B is only in your Honor's
11:34:52AM 12 binder, because it contains contraband.

11:34:56AM 13 MR. FIEMAN: We do need to see it.

11:35:01AM 14 MR. BECKER: Can I ask that we turn our monitors
11:35:04AM 15 just so it is not visible to the gallery? First, I would
11:35:18AM 16 move to admit 13B.

11:35:22AM 17 THE COURT: What is 13B? Agent Alfin, what is
11:35:33AM 18 13B?

11:35:36AM 19 THE WITNESS: I'm sorry, your Honor, I don't
11:35:38AM 20 recall off the top of my head. I can take a quick look at
11:35:40AM 21 your binder if you want me to.

11:35:56AM 22 MR. FIEMAN: Your Honor, I have had an opportunity
11:35:58AM 23 to look at it. I have no objection to its admission.

11:36:06AM 24 By Mr. Becker:

11:36:07AM 25 Q. Sorry, Special Agent Alfin. Are you able to see

11:36:11AM 1 Exhibit 13B?

11:36:13AM 2 A. I am now.

11:36:13AM 3 Q. What is it?

11:36:14AM 4 A. After the Website A was taken off line in March 2015,
11:36:21AM 5 an off-line version of the website was created, which is
11:36:24AM 6 available for review at an FBI facility. That website
11:36:29AM 7 depicts Website A as it appears when it was taken off
11:36:32AM 8 line. This is a screenshot from that recreated version of
11:36:36AM 9 Website A that depicts the specific post that the Pewter
11:36:42AM 10 user account accessed when the NIT collected the
11:36:45AM 11 information associated with the Pewter user account. It
11:36:49AM 12 shows a posting in the Preteen Videos - Girls Hardcore
11:36:55AM 13 section of Website A. And it contains --

11:36:58AM 14 Q. Sorry. What is the posting title?

11:37:00AM 15 A. The posting title is, "Girl 12ish eats other girls
11:37:06AM 16 slash dirty talk."

11:37:36AM 17 Q. Special Agent Alfin, to where was the data collected
11:37:41AM 18 by the NIT? Where was that returned to when it was
11:37:44AM 19 collected?

11:37:44AM 20 A. That data was returned to a computer controlled by
11:37:49AM 21 the FBI in the Eastern District of Virginia. A copy of
11:37:54AM 22 that data was then made available to me in my offices, as
11:37:57AM 23 well as my squad mates, in Linthicum, Maryland.

11:38:02AM 24 Q. Was that data then used to create the report that you
11:38:06AM 25 have testified to, Exhibit 15?

11:38:08AM 1 A. It was.

11:38:09AM 2 Q. And where was the website server of the website
11:38:25AM 3 located at the time that all of this activity was
11:38:27AM 4 occurring?

11:38:28AM 5 A. It was located on a government-controlled server --
11:38:31AM 6 computer server in the Eastern District of Virginia.

11:38:47AM 7 MR. BECKER: The court's brief indulgence, your
11:38:49AM 8 Honor.

11:39:26AM 9 By Mr. Becker:

11:39:29AM 10 Q. Special Agent Alfin, once the information was
11:39:32AM 11 returned -- the NIT information was returned to a
11:39:34AM 12 government computer, how, if at all, were agents able to
11:39:37AM 13 access it?

11:39:39AM 14 A. During the course of operating and monitoring
11:39:43AM 15 Website A, the information returned by the NIT was first
11:39:49AM 16 sent directly to a government computer in the Eastern
11:39:52AM 17 District of Virginia. That information was then
11:39:56AM 18 replicated to another server located at the major case
11:40:00AM 19 coordination unit in Linthicum, Maryland. That
11:40:04AM 20 information was there, available for review by the agents
11:40:06AM 21 who were monitoring the website 24 hours a day, seven days
11:40:10AM 22 a week, until the website was taken off line.

11:40:23AM 23 Q. In terms of the deployment of the NIT, was that --
11:40:28AM 24 you stated it occurred when the user clicked on that
11:40:31AM 25 particular message thread that you described. Was that an

11:40:35AM 1 active or passive process?

11:40:37AM 2 A. It was a passive process. The NIT was configured
11:40:41AM 3 such that when one user accessed the post, as the Pewter
11:40:47AM 4 account did, that the NIT would then be triggered and then
11:40:51AM 5 deployed. The FBI agents monitoring the website did not
11:40:55AM 6 need to take additional actions to deploy the NIT against
11:41:02AM 7 individual users.

11:41:03AM 8 Q. And why was that the case for the particular forum
11:41:07AM 9 that was navigated to by Pewter?

11:41:11AM 10 A. The NIT was deployed against users who accessed posts
11:41:18AM 11 in the Preteen Videos - Girls Hardcore forum because users
11:41:23AM 12 accessing posts in that forum were attempting to access or
11:41:29AM 13 distribute or advertise child pornography. At the point
11:41:35AM 14 where a user in that forum accessed a post, we can
11:41:40AM 15 affirmatively state that a user has attempted to access
11:41:44AM 16 child pornography.

11:41:50AM 17 Q. In terms of the information that was collected by the
11:41:52AM 18 NIT, was that ultimately --

11:41:54AM 19 THE COURT: The NIT did not just go to anyone that
11:41:59AM 20 logged into the website?

11:42:02AM 21 THE WITNESS: No, your Honor. The warrant did
11:42:04AM 22 authorize us to deploy the NIT in that fashion. And then
11:42:09AM 23 the FBI, as noted in the warrant, that we may further
11:42:15AM 24 restrict how we deploy the NIT, deployed it in such a
11:42:19AM 25 fashion that the NIT was deployed against users who

11:42:22AM 1 attempted to access illicit content.

11:42:28AM 2 THE COURT: So it was only attached to a
11:42:36AM 3 particular forum?

11:42:38AM 4 THE WITNESS: It was only deployed within certain
11:42:40AM 5 forums on the website, yes, your Honor.

11:42:43AM 6 THE COURT: Okay.

11:42:45AM 7 MR. BECKER: Your Honor, I can point to the
11:42:47AM 8 warrant affidavit. I will have an opportunity for that.
11:42:52AM 9 By Mr. Becker:

11:42:53AM 10 Q. Was the information collected by the NIT ultimately
11:42:55AM 11 provided to FBI in the Vancouver, Washington area?

11:43:00AM 12 A. It was.

11:43:00AM 13 Q. And just in summary, what actions were taken by FBI
11:43:13AM 14 in this area based on that information?

11:43:15AM 15 A. The major case coordination unit, after receiving the
11:43:19AM 16 information that was collected by the NIT, served a
11:43:25AM 17 subpoena to Comcast cable, which identified a residence in
11:43:32AM 18 Vancouver, Washington. That information, along with a
11:43:37AM 19 user report for the Pewter account, and other information
11:43:40AM 20 about the investigation, was provided to the Seattle FBI
11:43:44AM 21 office, which covers the Vancouver, Washington area.
11:43:48AM 22 Using that information, a search warrant was executed at
11:43:52AM 23 the defendant's residence.

11:43:54AM 24 Q. Was information pertaining to the -- information
11:43:59AM 25 collected by the NIT recovered from the home of the

11:44:02AM 1 defendant, Mr. Michaud?

11:44:03AM 2 A. Yes. Specifically the unique MAC address that was
11:44:08AM 3 identified by the NIT was found to be associated with a
11:44:13AM 4 particular network adapter that was recovered from the
11:44:16AM 5 defendant's residence.

11:44:19AM 6 Q. To your knowledge, was child pornography evidence
11:44:23AM 7 also recovered during that search?

11:44:24AM 8 A. Yes. I have read reports indicating that a large
11:44:29AM 9 quantity of child pornography, images, and videos were
11:44:35AM 10 recovered from digital devices in the defendant's
11:44:37AM 11 residence.

11:44:43AM 12 MR. BECKER: Your Honor, for the record, I think I
11:44:45AM 13 neglected to ask that 13B be filed under seal because of
11:44:49AM 14 contraband. I would make that request at this time.

11:44:51AM 15 THE COURT: Yeah, it should be under seal. If I
11:44:55AM 16 didn't say so, it may be admitted.

11:44:58AM 17 (Exhibit No. 13B was admitted.)

11:45:03AM 18 MR. BECKER: Does your Honor have further
11:45:04AM 19 questions for the government at this point?

11:45:09AM 20 THE COURT: Yeah, I do have one question, Agent
11:45:14AM 21 Alfin, and then the defense may have some questions for
11:45:16AM 22 you.

11:45:18AM 23 Is there any way for the FBI to go back down this NIT
11:45:30AM 24 to get into the subject computer, the user's computer?

11:45:37AM 25 THE WITNESS: No, your Honor. After the NIT

11:45:39AM 1 collected the limited amount of information that it was
11:45:43AM 2 permitted to collect, there was nothing that resided on
11:45:46AM 3 the subject's computer that would allow the government to
11:45:49AM 4 go back and further access that computer.

11:45:56AM 5 THE COURT: That answers my question, I guess.

11:46:03AM 6 MR. BECKER: Your Honor, I just want to -- before
11:46:13AM 7 I yield to the defense, your Honor, I did want to point
11:46:16AM 8 your Honor to the NIT search warrant. This is, again,
11:46:22AM 9 Exhibit 1 to Docket 47. It is Exhibit 1 in our exhibit
11:46:26AM 10 book.

11:46:27AM 11 THE COURT: What exhibit?

11:46:33AM 12 MR. BECKER: Exhibit 1 in the exhibit book.

11:46:35AM 13 THE COURT: What page?

11:46:37AM 14 MR. BECKER: Page 24, Footnote 8. I would point
11:46:59AM 15 the court to Footnote 8. Footnote 8 indicates, although
11:47:03AM 16 the application and affidavit, as it did, requests
11:47:06AM 17 authority to deploy to any user who logged in with a user
11:47:09AM 18 name and a password --

11:47:11AM 19 THE COURT: You are dropping your voice.

11:47:12AM 20 MR. BECKER: Sorry, your Honor. Just to make the
11:47:14AM 21 point that this footnote indicated that, although the
11:47:16AM 22 application was to deploy to any user who logged in with a
11:47:22AM 23 user name and a password, the affidavit does articulate
11:47:25AM 24 that the FBI may deploy in a more limited sort of fashion,
11:47:30AM 25 including in particular areas of the target website, such

11:47:34AM 1 as the target website sub-forums described in
11:47:39AM 2 Paragraph 27. And if your Honor looks at Paragraph 27,
11:47:49AM 3 and that is on Page 20 and Page 21, that includes the
11:48:05AM 4 sub-forum that we saw earlier, that is, Preteen Videos -
11:48:09AM 5 Girls Hardcore, the forum in which the defendant was
11:48:10AM 6 operating at the time that the NIT was deployed.

11:48:18AM 7 There is no question the warrant requested and was
11:48:22AM 8 granted authority to deploy to anyone who logged in with a
11:48:23AM 9 user name and password. In this instance that is how the
11:48:26AM 10 deployment occurred. Nothing further at this point, your
11:48:38AM 11 Honor.

11:48:39AM 12 THE COURT: Mr. Fieman.

11:48:44AM 13 CROSS-EXAMINATION

11:48:46AM 14 By Mr. Fieman:

11:48:56AM 15 Q. Good morning, Agent Alfin.

11:48:57AM 16 A. Good morning.

11:48:58AM 17 Q. I am Colin Fieman. I am one of Mr. Michaud's defense
11:49:02AM 18 attorneys. We haven't met before, have we?

11:49:04AM 19 A. Not formally.

11:49:06AM 20 Q. If there is anything I ask that isn't clear, and we
11:49:10AM 21 are in some confusing territory, please just ask me to
11:49:14AM 22 restate the question, okay?

11:49:16AM 23 A. Understood.

11:49:16AM 24 Q. Now, we have been going actually a couple of hours
11:49:19AM 25 now trying to sort out exactly what this NIT does, for

1 Judge Bryan. Do you know if Judge Buchanan had any
2 information or questions beyond what is in the warrant
3 about how this thing worked when the warrant was approved?

4 A. I am not aware whether or not Judge Buchanan asked
5 for any additional information beyond what was stated in
6 the warrant affidavit.

7 Q. Now, please bear with me, because we are all trying
8 to figure this out. I want to kind of go
9 step-through-step with kind of concrete imagery how a NIT
10 works. If you can guide me through that process, it will
11 be easier. Okay?

12 A. I will answer your questions.

13 Q. Now, the problem that the FBI faced when it was
14 investigating users of Site A was that you couldn't tell
15 who was signing into this site, because their identifying
16 information was masked, right?

17 A. That's correct.

18 Q. And that's because that is what the Tor browser or
19 the Tor network does, it strips out that IP address,
20 something like a phone number or an address, that would
21 normally be transmitted with the user accessing the site?

22 A. I would not agree with the statement that that
23 information is stripped out. I would agree that the Tor
24 network does obfuscate and make that information
25 difficult, if not impossible, to identify.

11:50:49AM 1 Q. So the problem you were trying to solve -- I say
11:50:54AM 2 "you," the FBI, was, how do we get the IP information when
11:50:59AM 3 it isn't sent to the website?

11:51:04AM 4 A. Some IP information is sent to the website, but that
11:51:09AM 5 IP information is not IP information that can be used to
11:51:12AM 6 identify the end-user.

11:51:14AM 7 Q. So basically people are calling into the website on
11:51:20AM 8 the Tor network, but you really can't see their telephone
11:51:23AM 9 numbers; is that fair?

11:51:25AM 10 A. I believe that's a fair analogy.

11:51:27AM 11 Q. So it is like a private caller. You want to know who
11:51:30AM 12 is calling the website, but you can't tell because the
11:51:32AM 13 number is not coming up? I understand that is loose.

11:51:38AM 14 A. I would agree with that characterization.

11:51:42AM 15 Q. So the point of the NIT then was that when -- at
11:51:47AM 16 least as far as the warrant authorized, somebody signed
11:51:49AM 17 into the website, somebody in Virginia could activate the
11:51:52AM 18 NIT, correct?

11:51:56AM 19 A. The NIT was not activated manually by an individual
11:52:01AM 20 in Virginia.

11:52:02AM 21 Q. Okay. So it was set up to activate automatically?

11:52:06AM 22 A. When certain conditions that were described in the
11:52:09AM 23 affidavit were met, yes.

11:52:11AM 24 Q. Such as signing into the website?

11:52:13AM 25 A. Yes.

11:52:13AM 1 Q. So at some point some FBI agent or tech specialist
11:52:18AM 2 set up the NIT to be activated when somebody signed in,
11:52:23AM 3 correct?

11:52:24AM 4 A. That's correct.

11:52:25AM 5 Q. And at the point that the person is signing in, and
11:52:30AM 6 the NIT is being activated, you don't have that telephone
11:52:33AM 7 number or complete IP address, correct? That's what you
11:52:36AM 8 want to get?

11:52:37AM 9 A. Prior to a user logging into the website, and prior
11:52:40AM 10 to the NIT being activated, we do not have any identifying
11:52:44AM 11 information, including an IP address, for that user.

11:52:48AM 12 Q. Correct. And the way the NIT works is that it is
11:52:53AM 13 then sent, without the user's knowledge, from the site in
11:52:57AM 14 Virginia to the user's computer, wherever that may be,
11:53:02AM 15 correct?

11:53:02AM 16 A. The user after certain conditions are met --

11:53:05AM 17 Q. Such as signing in?

11:53:06AM 18 A. Correct. As articulated in the warrant.

19 Q. Yes.

11:53:10AM 20 A. And in the case of this defendant, accessing a
11:53:13AM 21 particular post on the website. By accessing that post on
11:53:18AM 22 the website, that user has triggered actions that causes
11:53:21AM 23 his computer to download certain information from the
11:53:23AM 24 website. We configured the NIT to supplement the
11:53:26AM 25 information being downloaded by the user with the NIT

11:53:30AM 1 instructions.

11:53:31AM 2 Q. Okay. And, again, I need to go really slowly because
11:53:35AM 3 already we are using words like "supplement" that are a
11:53:37AM 4 little confusing. Just step-by-step. The user has signed
11:53:41AM 5 in, the FBI has set it up so the NIT will be deployed at
11:53:47AM 6 sign in, or at some other point, correct?

11:53:50AM 7 A. After certain conditions are met, yes.

11:53:53AM 8 Q. Then that NIT is really like a package of code or
11:53:56AM 9 data, right?

11:53:57AM 10 A. Yes.

11:53:58AM 11 Q. And when the user is signing in, they don't know that
11:54:03AM 12 they are getting that package of code or data sent to
11:54:06AM 13 them, right? The whole point is it is in the background,
11:54:09AM 14 and secret?

11:54:10AM 15 A. When the user downloads the NIT instructions to their
11:54:13AM 16 computer, it is intended to be invisible to the user.

11:54:16AM 17 Q. It is invisible. Okay. They are signing in and then
11:54:19AM 18 all of a sudden this thing in the background --
11:54:22AM 19 information is being sent from Virginia, to, in this case,
11:54:24AM 20 a Washington computer, by the FBI?

11:54:26AM 21 A. It is being downloaded from the server in the Eastern
11:54:30AM 22 District of Virginia by the user who has accessed the
11:54:33AM 23 website.

11:54:33AM 24 Q. How does the NIT code get from Virginia to
11:54:39AM 25 Washington? It travels, right?

11:54:41AM 1 A. Yes. It is downloaded to the user's computer after
11:54:45AM 2 logging into the website when they are using the password
11:54:47AM 3 and after certain conditions are met.

11:54:49AM 4 Q. So the NIT code travels from Virginia to the
11:54:52AM 5 Washington computer in this case, correct?

11:54:53AM 6 A. It does.

11:54:54AM 7 Q. And the user does not know that is happening. The
11:54:58AM 8 whole point is that is secret, correct?

11:55:00AM 9 A. Correct.

11:55:00AM 10 Q. So then when the NIT lands on the Washington
11:55:05AM 11 computer, it does certain things that the user is not
11:55:08AM 12 aware of, correct?

11:55:09AM 13 A. That's correct.

11:55:11AM 14 Q. What it does is it searches the user's computer, in
11:55:16AM 15 this case the Washington computer, to find that
11:55:20AM 16 identifying information, like the IP address, correct?

11:55:22AM 17 A. It instructs the user's computer to send the
11:55:25AM 18 information identified in the NIT warrant attachment to
11:55:30AM 19 the government-controlled computer, in addition to the
11:55:33AM 20 information that the user's computer was already sending
11:55:36AM 21 to the government-controlled computer.

11:55:38AM 22 Q. But we know the IP address, the identifying
11:55:40AM 23 information, is not being sent without that NIT, right?

11:55:43AM 24 A. The user's IP address is being transmitted across the
11:55:48AM 25 internet. But given the function of the Tor network, the

11:55:53AM 1 user's IP address during the normal course of operation of
11:55:57AM 2 a website that operates on the Tor network does not make
11:56:00AM 3 it to the government computer.

11:56:01AM 4 Q. Just to try and picture this. It is a little bit
11:56:05AM 5 like you have a police station -- FBI headquarters -- or,
11:56:08AM 6 excuse me, the FBI server in Virginia where the NIT is
11:56:13AM 7 stored and ready to go, right?

11:56:15AM 8 A. Our server that hosted Website A was in Virginia,
11:56:18AM 9 yes.

11:56:18AM 10 Q. And then somebody calls into that server, but he
11:56:24AM 11 can't see the number, so you send the NIT, like a police
11:56:28AM 12 officer or agent, out of Virginia, to the computer, to
11:56:31AM 13 find the IP address, correct?

11:56:32AM 14 A. I don't necessarily agree with the phone call
11:56:37AM 15 analogy, because anyone can call any phone number at any
11:56:40AM 16 given time. For the deployment of our NIT, you had to do
11:56:44AM 17 more than just call the website. Anyone could access the
11:56:47AM 18 front page of the website, and at that point the NIT would
11:56:50AM 19 not be deployed. They had to then log into the website
11:56:53AM 20 with a user name and password. So I want to make sure
11:56:56AM 21 that we are distinguishing the differences in the
11:56:59AM 22 analogies.

11:56:59AM 23 Q. I think that is a fair distinction. They have to
11:57:02AM 24 type in their user name and password on the homepage to
11:57:05AM 25 get that process?

11:57:06AM 1 A. Correct.

11:57:07AM 2 Q. Fair enough. So once that police officer, or in this
11:57:11AM 3 case the NIT, the undercover code, reaches Mr. Michaud's
11:57:16AM 4 home and his computer, it lands on his computer, and then
11:57:19AM 5 finds the IP address, and says send it back to Virginia,
11:57:22AM 6 correct?

11:57:22AM 7 A. I don't agree with the characterization of the NIT
11:57:27AM 8 code as being a police officer or undercover code. But I
11:57:32AM 9 can clarify anything that I have already stated about how
11:57:35AM 10 the NIT is delivered.

11:57:36AM 11 Q. So we know it is delivered to the computer in
11:57:39AM 12 Washington. And then when the IP address is sent back to
11:57:44AM 13 Washington -- It is stored there, right?

11:57:47AM 14 A. It is sent to Virginia.

11:57:48AM 15 Q. Sent to Virginia.

11:57:50AM 16 A. Where the NIT warrant was authorized.

11:57:52AM 17 Q. That is a little bit like an evidence room, right?
11:57:56AM 18 That data is securely stored and then agents can go in
11:57:59AM 19 later and retrieve it, look at it, and create all of these
11:58:03AM 20 spreadsheets that we have seen, correct?

11:58:04AM 21 A. The information was sent to a government-controlled
11:58:07AM 22 computer in the Eastern District of Virginia, and that
11:58:09AM 23 information was preserved as evidence.

11:58:11AM 24 Q. Now, Agent Alfin, just so we understand, you know, we
11:58:18AM 25 are talking about searches -- the search and the seizure,

11:58:22AM 1 exactly where the information -- the evidence is taken
11:58:24AM 2 from, correct? That is an issue that we are kind of
11:58:27AM 3 struggling with here, right?

11:58:29AM 4 A. I believe that is one of the questions that is being
11:58:32AM 5 answered today.

11:58:34AM 6 Q. Yes. Would you agree or disagree with various
11:58:38AM 7 statements in the government's pleading when it
11:58:40AM 8 characterizes the IP information as information seized
11:58:46AM 9 from Michaud's computer?

11:58:49AM 10 MR. BECKER: Objection. It is irrelevant. It is
11:58:53AM 11 asking for a legal conclusion, your Honor.

11:58:58AM 12 MR. FIEMAN: I am just asking if he agrees or
11:58:59AM 13 disagrees with that characterization.

11:58:59AM 14 THE COURT: Rephrase the question.

11:59:01AM 15 By Mr. Fieman:

11:59:02AM 16 Q. Do you agree or disagree with the statement that the
11:59:04AM 17 IP address, and all that they were talking about,
11:59:07AM 18 constitutes information seized from Michaud's computer?

11:59:12AM 19 MR. BECKER: Objection. Again, calling for a
11:59:13AM 20 legal conclusion.

11:59:14AM 21 THE COURT: I think you may answer.

11:59:16AM 22 THE WITNESS: Could you restate the question?

23 By Mr. Fieman:

11:59:19AM 24 Q. Do you agree or disagree with the statement that the
11:59:25AM 25 Department of Justice itself has made characterizing the

11:59:28AM 1 IP address and all this evidence as information seized
11:59:32AM 2 from Michaud's computer?

11:59:45AM 3 A. The information was reported by Mr. Michaud's
11:59:51AM 4 computer. My hesitation in giving a flat yes to that is
11:59:58AM 5 that an IP address is not necessarily assigned directly to
12:00:03PM 6 a computer, but it utilizes that IP address. I just want
12:00:07PM 7 to make sure that my answer is not misconstruing how the
12:00:11PM 8 internet and IP addresses work.

12:00:13PM 9 Q. Let me put it this way: If somebody -- Let's use
12:00:20PM 10 the telephone analogy. I know it is not perfect. If
12:00:23PM 11 somebody makes a phone call, and you have caller ID, you
12:00:25PM 12 can see their telephone number come up on your cellphone,
12:00:29PM 13 correct?

12:00:29PM 14 A. Correct.

12:00:29PM 15 Q. If you can't see the telephone number, because they
12:00:31PM 16 have a private caller or a number-blocking device, then
12:00:34PM 17 you can't see the telephone number just looking at your
12:00:36PM 18 phone, right?

12:00:37PM 19 A. Generally, yes.

12:00:38PM 20 Q. So what you might do, one alternative is, you might
12:00:40PM 21 say, well, we believe this person is engaged in criminal
12:00:42PM 22 activity, so we are going to go to his house, and we are
12:00:45PM 23 going to open the door and go inside and look at the
12:00:49PM 24 telephone number that he has written down in his address
12:00:51PM 25 book? That would be one way to get the telephone number,

12:00:54PM 1 correct?

12:00:54PM 2 A. I am not tracking in your example on how we have gone
12:00:58PM 3 from not knowing a person's phone number to being inside
12:01:01PM 4 their house.

12:01:03PM 5 Q. Withdrawn.

12:01:04PM 6 THE COURT: It is lunchtime, counsel. Let's just
12:01:07PM 7 take one hour. We have a ceremony at 4:00, the induction
12:01:17PM 8 of a new magistrate judge here. We are going to have to
12:01:23PM 9 stop at 3:30, 3:45 at the latest, this afternoon. Keep
12:01:30PM 10 your eye on the clock. You guys probably want to stay
12:01:34PM 11 here over the weekend, from what I understand about the
12:01:38PM 12 weather back east.

12:01:39PM 13 MR. BECKER: There is not going to be an option.

12:01:43PM 14 MR. FIEMAN: Dr. Soghoian is here. As I
15 indicated, he was supposed to be in Europe, and
12:01:49PM 16 rescheduled. He is supposed to be in Europe on Monday.
12:01:51PM 17 What we would ask is, if maybe we could avail other
12:01:57PM 18 witnesses, I could finish with Agent Alfin, that will take
12:01:59PM 19 about 15 minutes --

12:02:00PM 20 THE COURT: Talk to counsel about that. It
12:02:02PM 21 doesn't matter to me whether you take witnesses out of
12:02:05PM 22 order. I am not sure that we have a lot more witnesses.
12:02:11PM 23 I understand this better now.

12:02:12PM 24 MR. FIEMAN: Thank you, your Honor.

01:06:50PM 25 (Lunch break.)

01:06:50PM 1 THE COURT: Agent Alfin, do you want to resume the
01:06:56PM 2 witness stand?

01:06:56PM 3 THE WITNESS: Yes, your Honor.

01:06:59PM 4 By Mr. Fieman:

01:07:05PM 5 Q. Agent Alfin, I just have one more quick question
01:07:09PM 6 about the NIT, and then I am going to wrap up with a few
01:07:11PM 7 questions about one other matter. Okay?

01:07:16PM 8 A. Okay.

01:07:17PM 9 Q. I just wanted to clarify, after the IP address and
01:07:20PM 10 other identifying information was sent to the FBI, you
01:07:24PM 11 then used that information to go to Comcast and get an
01:07:28PM 12 address and all that stuff that would help you locate
01:07:32PM 13 physical addresses from the IP address, correct?

01:07:35PM 14 A. That is correct. The IP address itself alerts us to
01:07:39PM 15 the fact that the subscriber is likely in the Vancouver,
01:07:45PM 16 Washington area, and you can use publicly available
01:07:48PM 17 databases to check that information, but we do serve a
01:07:51PM 18 subpoena to Comcast to identify the actual subscriber.

01:07:53PM 19 Q. So why didn't you just go to Comcast originally when
01:07:56PM 20 you saw Pewter signing into the website?

01:08:01PM 21 A. During the normal course of operation, the website
01:08:05PM 22 that operates on the Tor network, the user's true IP
01:08:08PM 23 address is not visible to the website.

01:08:10PM 24 Q. It is only after the IP address was sent to Virginia
01:08:13PM 25 from the computer that you were able to go to Comcast,

01:08:16PM 1 correct?

01:08:16PM 2 A. That's correct.

01:08:17PM 3 Q. Now, previously -- Now, we are moving on to a little
01:08:24PM 4 bit, briefly, about the website itself. You looked
01:08:27PM 5 previously at Government Exhibit 12A. Do you have that in
01:08:30PM 6 front of you?

01:08:30PM 7 A. I am pulling it up now. I have it in front of me.

01:08:42PM 8 Q. You have seen that photograph before. You are
01:08:46PM 9 familiar with the record in this case, correct?

01:08:47PM 10 A. I am.

01:08:48PM 11 Q. And that 12A is a shot of the website's homepage, the
01:08:55PM 12 log-in page; is that correct?

01:08:56PM 13 A. Yes.

01:08:57PM 14 Q. And do you notice down somewhere in the lower right
01:09:05PM 15 corner there is a date?

01:09:06PM 16 A. Yes.

01:09:06PM 17 Q. And what is the date?

01:09:07PM 18 A. February 3rd, 2015.

01:09:09PM 19 Q. So that Government 12A depicts the homepage as it
01:09:17PM 20 appeared approximately 17 days before the search warrant
01:09:21PM 21 application, correct?

01:09:22PM 22 A. That's correct.

01:09:22PM 23 Q. Because the search warrant was obtained on
01:09:27PM 24 February 20th, 2015?

01:09:28PM 25 A. The NIT search warrant?

01:09:29PM 1 Q. The NIT search warrant, yes.

01:09:31PM 2 A. Correct.

01:09:32PM 3 Q. Can you now turn to -- I am going to show you what
01:09:41PM 4 has been marked as Defense Exhibits A15 and A16.

01:09:46PM 5 If I may approach, your Honor? We just supplied
01:09:54PM 6 these exhibits to you.

01:09:59PM 7 Agent Alfin, I believe those are just additional
01:10:01PM 8 copies of what is already in Government Exhibit 14, just
01:10:04PM 9 so the record is clear. Is that right?

01:10:06PM 10 A. Let me verify what is in Government 14. Yes, these
01:10:17PM 11 appear to be the same images.

01:10:19PM 12 Q. Now, it is correct that -- Actually, these two
01:10:22PM 13 pictures depict a laptop that I believe was seized in
01:10:29PM 14 Naples, Florida, on February 19th, 2015; is that correct?

01:10:32PM 15 A. I believe the search warrant record reflects that the
01:10:37PM 16 laptop was actually seized on February 20th.

01:10:40PM 17 Q. We will look for the search -- That is in the search
01:10:44PM 18 warrant application, correct? Would that refresh your
01:10:47PM 19 recollection on the date that the Naples, Florida search
01:10:52PM 20 was executed? Could you take a look at that?

01:10:54PM 21 A. The beginning of the execution of the warrant did
01:10:56PM 22 occur on the 19th. I just want to clarify that we exited
01:11:00PM 23 the residence on February 20th. That would be the time
01:11:03PM 24 the actual laptop would have been seized.

01:11:05PM 25 Q. Okay. And when we are talking about the Naples,

01:11:08PM 1 Florida residence, we are talking about the residence of
01:11:11PM 2 the original operator or administrator of this site, or
01:11:15PM 3 one of the operators; is that correct?

01:11:17PM 4 A. That's correct.

01:11:18PM 5 Q. And what was his name, do you recall?

01:11:22PM 6 MR. BECKER: Objection to relevance.

01:11:28PM 7 By Mr. Fieman:

01:11:30PM 8 Q. You are familiar with the photographs that were taken
01:11:33PM 9 in Naples, Florida, correct?

01:11:34PM 10 A. Yes, I was present for the execution of that search
01:11:36PM 11 warrant.

01:11:37PM 12 Q. So you were present. Now, I would like you to turn
01:11:39PM 13 to Government 14. It is the second picture that shows a
01:11:47PM 14 banner in a little bit of detail for Playpen; is that
01:11:52PM 15 correct? It says in the upper left-hand corner, "Playpen
01:11:55PM 16 welcomes you"?

01:11:56PM 17 A. It does.

01:11:57PM 18 MR. FIEMAN: Your Honor, do you have that exhibit?

01:11:58PM 19 THE COURT: I don't know what you are talking
01:12:00PM 20 about. Are you talking about A14?

01:12:03PM 21 MR. FIEMAN: Government 14, your Honor.

01:12:10PM 22 THE COURT: That is the, "Use of cell-site
01:12:14PM 23 simulator technology"?

01:12:17PM 24 MR. FIEMAN: Government 14 should be two pictures
01:12:19PM 25 of a laptop, your Honor.

01:12:20PM 1 THE COURT: That is 15 and 16.

01:12:27PM 2 THE CLERK: He is in the government's.

01:12:27PM 3 MR. FIEMAN: That's fine. The defense exhibits
01:12:29PM 4 are the same.

01:12:31PM 5 By Mr. Fieman:

01:12:31PM 6 Q. Let me refer then to A15 and 16 -- Defense A15 and
01:12:37PM 7 A16. Those show the website as it appeared on
01:12:44PM 8 February 19th or on the morning of February 20th; is that
01:12:48PM 9 correct?

01:12:48PM 10 A. That's correct.

01:12:49PM 11 Q. And those pictures were taken as you were -- the FBI
01:12:53PM 12 was in fact in the process of seizing the control of the
01:12:57PM 13 website, correct?

01:12:59PM 14 A. It happened in a similar -- closely-related
01:13:02PM 15 timeframe, yes.

01:13:02PM 16 Q. And then shortly afterwards, on the 20th, the NIT
01:13:06PM 17 warrant application was completed and presented to the
01:13:09PM 18 judge in Virginia, correct?

01:13:11PM 19 A. That is correct.

01:13:11PM 20 Q. So now you can see in the upper left-hand corner that
01:13:15PM 21 there is a logo that appears there?

01:13:17PM 22 A. Yes, there is.

01:13:18PM 23 Q. And do you see any lascivious display of prepubescent
01:13:24PM 24 girls in that left corner?

01:13:26PM 25 A. The logo depicted in this image depicts what appears

01:13:30PM 1 to be a prepubescent female posed in a sexually suggestive
01:13:35PM 2 manner.

01:13:36PM 3 Q. Do you see any nudity or -- Do you see two females
01:13:41PM 4 anywhere there?

01:13:41PM 5 A. I do not.

01:13:42PM 6 Q. Do you see their legs spread apart?

01:13:45PM 7 A. I do not.

01:13:46PM 8 Q. It is fair to say that the February 3rd logo that we
01:13:50PM 9 saw earlier did not exactly match what you seized on the
01:13:53PM 10 19th, correct?

01:13:54PM 11 A. The logo did change.

01:13:56PM 12 Q. At any point is the warrant application amended or
01:14:02PM 13 corrected to change the description of the images that
01:14:08PM 14 appeared with the logo?

01:14:09PM 15 A. The warrant for the NIT reflected a specific period
01:14:14PM 16 of review, and it was not updated to include my
01:14:17PM 17 observations from the night of February 19th and morning
01:14:20PM 18 of February 20th.

01:14:23PM 19 MR. FIEMAN: Thank you. That is all the questions
01:14:24PM 20 I have.

01:14:36PM 21 MR. BECKER: Your Honor, may I redirect Special
01:15:02PM 22 Agent Alfin pertaining to this issue, which was -- Thank
01:15:04PM 23 you.

01:15:04PM 24 REDIRECT EXAMINATION

01:15:05PM 25 By Mr. Becker:

01:15:06PM 1 Q. Special Agent Alfin, did there come a point in time
01:15:09PM 2 where the administrator changed, as you testified about,
01:15:11PM 3 the logo of the website?

01:15:13PM 4 A. Yes.

01:15:13PM 5 Q. And when did that occur, based on examination of the
01:15:17PM 6 website?

01:15:17PM 7 A. It occurred approximately in the early evening hours
01:15:21PM 8 of February 19th, several hours before his arrest.

01:15:25PM 9 Q. Was there a posting on the website that reflected
01:15:28PM 10 that?

01:15:28PM 11 A. There was a posting in the administration section of
01:15:32PM 12 the website, indicating that the administrator had changed
01:15:35PM 13 the logo.

01:15:36PM 14 Q. Can I refer you and ask you to review Exhibit 12D?

01:15:56PM 15 A. I have the exhibit in front of me.

01:15:58PM 16 Q. What is Exhibit 12D? Excuse me. I'm sorry. Please
01:16:11PM 17 review Exhibit 13A. My apologies.

01:16:17PM 18 A. I have the exhibit in front of me.

01:16:20PM 19 Q. What is Exhibit 13A?

01:16:22PM 20 A. Exhibit 13A is a posting from the administration
01:16:28PM 21 section of Website A. The post is entitled, "Logo
01:16:33PM 22 Contest." And it has a discussion between various
01:16:37PM 23 administrators and moderators of Website A about changing
01:16:40PM 24 the logo of Website A.

01:16:46PM 25 MR. BECKER: Move Exhibit 13A into evidence, your

01:16:50PM 1 Honor.

01:16:50PM 2 MR. FIEMAN: No objection.

01:16:50PM 3 THE COURT: It may be admitted.

01:16:52PM 4 (Exhibit No. 13A was admitted.)

01:16:52PM 5 By Mr. Becker:

01:16:52PM 6 Q. If I can direct your attention to the last page of
01:16:56PM 7 Exhibit 13A?

01:16:59PM 8 A. I have it in front of me.

01:17:01PM 9 Q. And is there a posting that indicates when the
01:17:05PM 10 administrator put the new logo onto the website?

01:17:08PM 11 A. There is. There is a posting in this thread created
01:17:11PM 12 by the primary administrative account that states, "I just
01:17:15PM 13 put it up." That posting, according to the website, is
01:17:19PM 14 dated February 20th, 2015. In actuality, that occurred
01:17:25PM 15 sometime on February 19th, 2015. The time discrepancy is
01:17:30PM 16 because the time zone of the website was several hours
01:17:33PM 17 ahead of eastern time.

01:17:35PM 18 Q. In terms of the -- You reviewed the two images on
01:17:47PM 19 the initial logo just a few moments ago; is that right?

01:17:49PM 20 A. Yes.

01:17:50PM 21 Q. When was the first time that you reviewed, to your
01:17:56PM 22 recollection, the website in question?

01:17:57PM 23 A. The first time that I reviewed the website in
01:18:01PM 24 question would have been approximately August 2014, after
01:18:06PM 25 it came online.

01:18:07PM 1 Q. And at that time what images were present on the logo
01:18:10PM 2 of the site?

01:18:11PM 3 A. Every time that I reviewed the website, between my
01:18:16PM 4 first viewing of it up until the execution of the search
01:18:20PM 5 warrant at the administrator's residence, it featured the
01:18:26PM 6 original logo, the one that was described in the warrant
01:18:29PM 7 affidavit, that featured what appeared to be two
01:18:34PM 8 prepubescent females.

01:18:36PM 9 Q. At the time you were in the home of the
01:18:38PM 10 administrator, do you recall taking particular notice of
01:18:41PM 11 any change to the website's logo?

01:18:44PM 12 A. No. At the time, while I would have clearly seen the
01:18:47PM 13 website and would have seen the new logo, it did not jump
01:18:50PM 14 out to me as a significant change to the website or a
01:18:52PM 15 material change to the website, given the content of the
01:18:55PM 16 logo and its similarity to the previous logo.

01:18:58PM 17 Q. Was it your intent that the change to the logo be
01:19:03PM 18 omitted from the NIT warrant in any way?

01:19:05PM 19 A. Absolutely not.

01:19:06PM 20 Q. Special Agent Alfin, just a few brief questions about
01:19:31PM 21 how a user communicates with a website, to go briefly back
01:19:35PM 22 to that topic. When a user communicates with a website,
01:19:39PM 23 such as the one in this case, what sort of information
01:19:42PM 24 does that user send to the website?

01:19:47PM 25 A. During the normal course of operation of a website,

01:19:50PM 1 such as Website A, when a user accesses the website, and
01:19:55PM 2 then logs into the website, they are sending various
01:19:59PM 3 pieces of information to that website. That information
01:20:02PM 4 includes information about processes running on the user's
01:20:06PM 5 computer. It also includes requests for information from
01:20:10PM 6 the website. During the normal course of operation, that
01:20:13PM 7 website responds by sending information back to the user's
01:20:18PM 8 computer, and that user can view that information inside
01:20:21PM 9 of a web browser. That information is typically displayed
01:20:25PM 10 as text information or graphical information. And while
01:20:29PM 11 the user remains connected to the website, that ongoing
01:20:32PM 12 exchange of information continues between the user's
01:20:35PM 13 computer and the website.

01:20:36PM 14 Q. So the user's computer is sending information to the
01:20:39PM 15 website, and the website is sending information back to
01:20:41PM 16 the user?

01:20:42PM 17 A. That is correct.

01:20:42PM 18 Q. Whether or not there has been any sort of NIT
01:20:46PM 19 installed on the website?

01:20:46PM 20 A. Correct.

01:20:47PM 21 Q. And is that the case for websites on Tor as well as
01:20:50PM 22 websites on the regular internet?

01:20:52PM 23 A. That's correct.

01:20:52PM 24 Q. And when a user clicks on a link on a website, what
01:20:59PM 25 is happening in the background in order for the user to

then go to the next part of that site?

A. When a user clicks on a link within a website, the user's computer sends a request to the website to send that particular page of the website back to the user's computer. Typically the website -- the computer server hosting the website will respond to that request by sending the requested information to the user's computer.

MR. BECKER: Thank you, your Honor. No further questions.

MR. FIEMAN: Some very brief follow-up on this issue.

RE CROSS-EXAMINATION

By Mr. Fieman:

Q. Agent Alfin, could you turn to Defense Exhibit A8? Do you have that defense binder in front of you?

A. I will pull it up now. I have it in front of me.

Q. And that reflects an email chain between myself, Assistant United States Attorney Kate Vaughan, Sam Mautz, who is an FBI agent, correct?

A. That's correct.

Q. And yourself?

A. That's correct.

Q. You may not have been aware at the time, but at some point you became aware that the defense and the United States Attorney's Office had a discovery conference in

01:22:27PM 1 Seattle in early November; is that correct?

01:22:29PM 2 A. I am aware that discovery material was turned over to
01:22:32PM 3 defense at various points in time.

01:22:34PM 4 Q. And you are aware that, according to this email chain
01:22:39PM 5 that you received and recollect, there was initially a
01:22:45PM 6 communication from me to Kate Vaughan regarding the
01:22:49PM 7 homepage and screenshots -- or just the pictures that we
01:22:53PM 8 are showing of the homepage; is that correct?

01:22:56PM 9 MR. BECKER: Object to relevance and personal
01:22:58PM 10 knowledge, your Honor.

11 MR. FIEMAN: Your Honor, he said that he is
01:23:02PM 12 familiar with the picture.

01:23:02PM 13 THE COURT: It is a fair objection. I don't know
01:23:04PM 14 what you're asking him here.

01:23:08PM 15 By Mr. Fieman:

01:23:09PM 16 Q. At some point on November 10th did Agent Mautz
01:23:14PM 17 contact you about producing a copy of the screen page --
01:23:17PM 18 the homepage -- a screenshot of the homepage? If you look
01:23:23PM 19 on the first page of A08?

01:23:25PM 20 A. Yes, he did contact me.

01:23:26PM 21 Q. And he asked you to send a new or different copy of
01:23:32PM 22 the homepage than had originally been produced for the
01:23:36PM 23 defense; is that correct?

01:23:37PM 24 A. This email chain doesn't specify exactly which images
01:23:43PM 25 that I sent to Special Agent Mautz, but I did send him

01:23:50PM 1 images.

01:23:51PM 2 Q. And Agent Mautz was following up with you on
01:23:54PM 3 November 10th, according to the 6:30 p.m. message,
01:23:58PM 4 because, as you can see below, "Defense is taking note of
01:24:05PM 5 the capture dates." Do you see that communication?

01:24:07PM 6 A. Just to clarify, you said that Agent Mautz was
01:24:10PM 7 following up with me, but that appears to be the first
01:24:12PM 8 time that he contacted me in this chain of email
01:24:15PM 9 communications.

01:24:15PM 10 Q. Okay. Had he contacted you previously about
01:24:18PM 11 obtaining a screenshot of the homepage?

01:24:21PM 12 A. Not that I recall.

01:24:22PM 13 Q. So at this point he is contacting you for the first
01:24:27PM 14 time to get a copy of the screen -- of the homepage, is
01:24:30PM 15 that correct, to the best of your recollection?

01:24:31PM 16 A. To the best of my recollection, yes.

01:24:33PM 17 Q. And he is doing that, he indicates, because "Defense
01:24:36PM 18 is taking note of the capture dates"?

01:24:40PM 19 A. Yes, he says that in his email.

01:24:42PM 20 Q. And when we refer to the capture dates, we are
01:24:46PM 21 talking about the date that particular homepage or image
01:24:50PM 22 was actually posted or appeared, correct?

01:24:52PM 23 A. I assume he was referring to material that was
01:24:54PM 24 provided to defense in earlier discovery reviews.

01:24:58PM 25 MR. FIEMAN: Thank you very much. No further

01:25:00PM 1 questions, your Honor.

01:25:00PM 2 THE COURT: Thank you, Agent Alfin. You may be
01:25:06PM 3 excused.

01:25:21PM 4 MR. BECKER: Your Honor, other than to ask the
01:25:23PM 5 admission of some exhibits just to clarify the record, we
01:25:26PM 6 don't have other witnesses to present, unless your Honor
01:25:28PM 7 has further questions to be addressed.

01:25:29PM 8 THE COURT: No, I don't.

01:25:31PM 9 MR. FIEMAN: No objection, your Honor, to
01:25:33PM 10 admission of everything that has been offered.

01:25:35PM 11 THE COURT: What now?

01:25:36PM 12 MR. FIEMAN: No objection to the admission of
01:25:39PM 13 everything that has been offered.

01:25:39PM 14 THE COURT: I don't know what has been offered.

01:25:50PM 15 MR. BECKER: Your Honor, for purposes of the
01:25:52PM 16 record, first we would offer Exhibits 1 through 9 on our
01:25:57PM 17 exhibit list. Each one of those exhibits is attached as
01:26:01PM 18 an exhibit to our previous filings. I just wanted to do
01:26:05PM 19 so for completion of the record.

01:26:08PM 20 MR. FIEMAN: No objection, your Honor.

01:26:09PM 21 THE COURT: They may be admitted.

01:26:15PM 22 (Exhibit Nos. 1 - 9 were admitted.)

01:26:15PM 23 MR. BECKER: And we would move for the admission
01:26:17PM 24 of the following: 12A, 12B, 13A, 13B, which we would ask
01:26:26PM 25 under seal because of contraband, 15, 15A, 15B. At this

01:26:42PM 1 time we would move for the admission of those for the
01:26:44PM 2 record.

01:26:46PM 3 MR. FIEMAN: Your Honor, I have no objection. But
01:26:47PM 4 we should also move in 14, which is the same as Defense
01:26:52PM 5 Exhibit A15 and A16. I would move for the admission of
01:26:56PM 6 all of those --

01:26:56PM 7 THE COURT: What numbers now? A15 and A16?

01:27:03PM 8 MR. FIEMAN: Yes, your Honor.

01:27:04PM 9 THE COURT: Do you have any objection to those?

01:27:05PM 10 MR. BECKER: No, your Honor.

01:27:07PM 11 THE COURT: All of those exhibits may be admitted.

01:27:13PM 12 (Exhibit Nos. A15 & A16 were admitted.)

01:27:13PM 13 MR. BECKER: One other issue, your Honor.
01:27:21PM 14 Exhibits 1 through 5 are all documents that are currently
01:27:24PM 15 under seal. We haven't had an opportunity to conference
01:27:26PM 16 with the defense in order to work out those issues, which
01:27:29PM 17 we will.

01:27:29PM 18 THE COURT: They should remain under seal until we
01:27:31PM 19 resolve that issue.

01:27:33PM 20 MR. BECKER: That would be our request. We will
01:27:34PM 21 confer on that issue.

01:27:41PM 22 MR. FIEMAN: Your Honor, if the government is
01:27:43PM 23 complete, we would call Dr. Chris Soghoian.

24 CHRIS SOGHOIAN

01:28:11PM 25 Having been sworn under oath, testified as follows:

DIRECT EXAMINATION

By Mr. Fieman:

Q. Dr. Soghoian, please spell your name for the record.

A. Sure. My name is Christopher Soghoian. That is C-H-R-I-S-T-O-P-H-E-R, Soghoian, S-O-G-H-O-I-A-N.

Q. And where do you work?

A. I am the principal technologist for the Speech Privacy and Technology Project at the American Civil Liberties Union. Although I should clarify, I am actually volunteering here in my personal capacity.

Q. Correct. We retained you as a technology expert in this case some time ago, correct?

A. That's correct.

Q. And are you being paid for your assistance?

A. I am being reimbursed for my flights, and my hotel, and a per diem for food, but that's it.

Q. What is your training and qualifications?

A. I have a bachelor's degree in computer science from James Madison University. I have a master's degree in computer security from Johns Hopkins University. I have a Ph.D. in informatics, which is like a mix of computer science and law, from Indiana University. And I specialized there in studying the role that the telephone companies play in enabling government surveillance.

Q. And have you testified in other court proceedings?

01:29:27PM 1 **A. This is my first appearance in court, but I have**
01:29:31PM 2 **acted as a defense expert for the public defender in**
01:29:34PM 3 **Spokane, Washington. I have also -- I also have quite a**
01:29:38PM 4 **bit of experience in training judges and explaining things**
01:29:41PM 5 **to judges. I appeared at an event organized by the**
01:29:45PM 6 **Federal Judicial Center in Washington, D.C. last year,**
01:29:48PM 7 **explaining surveillance technology to judges. I also**
01:29:51PM 8 **spoke to 60 Article III judges last year at an event**
01:29:56PM 9 **organized by Georgetown Law School.**

01:29:59PM 10 **Q. Slow down a little bit so the court reporter can get**
01:30:02PM 11 **everything. You have also testified before the advisory**
01:30:05PM 12 **committee on the Federal Rules of Criminal Procedure?**

01:30:07PM 13 **A. I have, yes, sir.**

01:30:09PM 14 **Q. And when did you do that?**

01:30:10PM 15 **A. I think that was in the fall of 2014.**

01:30:14PM 16 **Q. And have you ever had your publications or scholarly**
01:30:17PM 17 **work cited by a court?**

01:30:19PM 18 **A. Yes. My research and scholarship has been cited by**
01:30:24PM 19 **several federal courts, including the dissent by the Chief**
01:30:28PM 20 **Judge of the Ninth Circuit, Alex Kozinski. My research**
01:30:32PM 21 **has also been cited by the state supreme court of**
01:30:35PM 22 **New Jersey and the state supreme court of Massachusetts.**

01:30:37PM 23 **Q. Now, as a consultant in this case, have you reviewed**
01:30:41PM 24 **the discovery and materials that relate to Mr. Michaud's**
01:30:46PM 25 **case?**

01:30:46PM 1 A. I have reviewed all documents you have sent to me,
01:30:49PM 2 yes.

01:30:49PM 3 Q. Did that, for example, include the NIT warrant
01:30:52PM 4 application?

01:30:53PM 5 A. I have reviewed the NIT warrant application, yes.

01:30:56PM 6 Q. Let me just cut to the chase. Would you please
01:30:58PM 7 explain to the judge what an NIT is and how it works?

01:31:01PM 8 A. Sure.

01:31:02PM 9 MR. BECKER: Objection, your Honor.

01:31:03PM 10 THE COURT: Wait a minute. I didn't get the
01:31:05PM 11 question.

01:31:06PM 12 MR. FIEMAN: I asked him to explain to the court
01:31:07PM 13 what an NIT is and how does it work.

01:31:12PM 14 MR. BECKER: I would object to the foundation and
01:31:15PM 15 speculation, your Honor. If this isn't based on any
01:31:17PM 16 analysis of a network investigative technique in this
01:31:20PM 17 case, i.e., the NIT in this case --

01:31:23PM 18 THE COURT: A little more foundation is
01:31:24PM 19 appropriate.

01:31:25PM 20 By Mr. Fieman:

01:31:25PM 21 Q. Dr. Soghoian, in the course of reviewing the
01:31:29PM 22 discovery, have you, for example, reviewed all of the
01:31:33PM 23 government's descriptions of the NIT that was deployed in
01:31:38PM 24 this case?

01:31:39PM 25 A. I have read the description of the NIT in this

01:31:42PM 1 warrant, and I have also read the description of the NIT
01:31:44PM 2 in every public NIT application that is available -- that
01:31:49PM 3 has become available over the last five or six years.

01:31:52PM 4 Q. When you talk about NIT, that is a kind of term of
01:31:57PM 5 art. It refers in the technology world to a specific type
01:32:01PM 6 of code or technique; is that correct?

01:32:02PM 7 A. The government describes this technology as a NIT.
01:32:06PM 8 In the computer security community, which I am part of,
01:32:09PM 9 this is generally described as malware or malicious
01:32:13PM 10 software.

01:32:13PM 11 Q. Can you explain what those are and why you describe
01:32:18PM 12 it as malware?

01:32:20PM 13 MR. BECKER: Objection, again, to the relevance of
01:32:23PM 14 the characterization, your Honor. We are not talking
01:32:25PM 15 about review of anything that actually happened in this
01:32:27PM 16 case, the NIT in this case. We are talking now based on
01:32:31PM 17 the witness' opinion and characterizations of how things
01:32:35PM 18 can be labeled. I don't see how this has any weight or
01:32:39PM 19 pertinence to the issues the court has to decide here. If
01:32:41PM 20 the witness has examined something that was used in this
01:32:44PM 21 case, as opposed to reading the documents, I might not
01:32:48PM 22 object.

01:32:48PM 23 THE COURT: I take this to be preliminary.
01:32:51PM 24 Obviously, it needs to be tied up with the evidence in
01:32:55PM 25 this case.

01:32:56PM 1 By Mr. Fieman:

01:32:56PM 2 Q. Let's use the word NIT. Does NIT have a meaning in
01:33:00PM 3 the technology and cybersecurity world?

01:33:03PM 4 A. I have been studying the government's use of what we
01:33:09PM 5 now know to be NITs for several years. We did not know
01:33:12PM 6 they called them NITs until we found one of the warrant
01:33:17PM 7 applications a couple of years ago. But this general
01:33:19PM 8 category of technology --

01:33:21PM 9 Let me pause and say the FBI is not the only
01:33:24PM 10 government agency in the world that seeks to use
01:33:28PM 11 investigative techniques of this kind. There are many
01:33:31PM 12 governments around the world that use techniques like
01:33:33PM 13 this, and there are many companies that create
01:33:36PM 14 special-purpose technology like this for these
01:33:40PM 15 governments. These companies advertise these products,
01:33:42PM 16 they advertise their features, they describe it in quite
01:33:45PM 17 extensive detail.

01:33:46PM 18 And so I have been researching this general category
01:33:49PM 19 of technology for a number of years, and I can describe,
01:33:53PM 20 again, in general terms, how it works. There are --
01:33:57PM 21 Within the class of what the government calls NITs, there
01:34:00PM 22 might be different kinds of NITs. Some NITs might do a
01:34:03PM 23 very small subset of things, some might do more things.
01:34:06PM 24 But I can tell you generally how these things work.

01:34:09PM 25 The reason that people in the computer security

01:34:12PM 1 community describe this as malware is that -- Computers
01:34:15PM 2 are built with cybersecurity protections within them.
01:34:18PM 3 When you are browsing around on the internet, and you
01:34:21PM 4 visit a website, under normal circumstances that website
01:34:24PM 5 is only allowed to get your computer to do certain things.
01:34:29PM 6 Malicious software, known as malware, tries to get your
01:34:32PM 7 computer to do things that it would not ordinarily do.

01:34:36PM 8 And in the case of this Tor software that we are
01:34:40PM 9 discussing here in this case -- I have been
01:34:44PM 10 researching -- I know the people who are behind the Tor
01:34:46PM 11 Project. They are academics. They go to the same
01:34:49PM 12 conferences -- the same academic conferences that I do.
01:34:53PM 13 This is a ten-year-old project that has received millions
01:34:55PM 14 of dollars of research funds to build a very secure piece
01:34:59PM 15 of software that has one primary purpose, which is to hide
01:35:02PM 16 the identity of people using it.

01:35:05PM 17 Q. Let's slow down. Now you are talking about the Tor
18 network, in general, correct?

19 A. Yes.

01:35:09PM 20 Q. Let's stop there. So you have been studying NITs for
01:35:13PM 21 a considerable period of time, you have done research on
01:35:16PM 22 it, and you have also reviewed all of the discovery in
01:35:18PM 23 this case, correct?

01:35:19PM 24 A. That's correct.

01:35:19PM 25 Q. Now, you have also seen the various pleadings that

01:35:22PM 1 the government has filed where they describe the NIT as
01:35:27PM 2 seizing information from Mr. Michaud's computer?

01:35:29PM 3 A. I have read that, yes, sir.

01:35:30PM 4 Q. Can you just describe for the judge the process of
01:35:34PM 5 how a NIT goes about doing that, in general layman's
01:35:38PM 6 terms, without getting into any technical features, just
01:35:43PM 7 in a bread-and-butter way how does that work?

01:35:45PM 8 MR. BECKER: Objection, your Honor. I would renew
01:35:48PM 9 my objection, your Honor. This is a lay witness'
01:35:51PM 10 interpretation of the words and warrants in discovery. It
01:35:55PM 11 is not based on any actual analysis of anything in this
01:35:58PM 12 case. This is testimony that is of no value to this court
01:36:00PM 13 in determining any of the issues here. We have made
01:36:03PM 14 disclosure of certain technical information about the
01:36:06PM 15 network investigative technique. If that's what the
01:36:10PM 16 witness has reviewed, then fine. But right now we are
01:36:13PM 17 just talking about looking at the legal documents. This
01:36:17PM 18 witness' opinion about what legal terms mean -- or what
01:36:20PM 19 terms in legal documents mean, again, I think this is
01:36:24PM 20 irrelevant information that does nothing in order to
01:36:26PM 21 illuminate any of the issues before the court.

01:36:28PM 22 THE COURT: I think your objection goes to the
01:36:31PM 23 weight to be attached. Go ahead.

01:36:35PM 24 By Mr. Fieman:

01:36:35PM 25 Q. Let's take up that objection for a moment. Have you

01:36:37PM 1 consulted with another expert retained by the defense
01:36:40PM 2 called Vlad Cirkovic?

01:36:44PM 3 A. I have spoken to Vlad.

01:36:46PM 4 Q. You are aware that we had actually requested from the
01:36:48PM 5 government the entire NIT code, so you could do exactly
01:36:52PM 6 the type of analysis that Mr. Becker says you have not
01:36:55PM 7 done?

01:36:56PM 8 A. It is true that if we had the complete code, that we
01:36:59PM 9 would know a lot more than we know right now.

01:37:01PM 10 Q. But based upon your consultations with Mr. Cirkovic
01:37:07PM 11 as to the limited code that has been turned over by the
01:37:09PM 12 government, and your extensive ten years of research into
01:37:12PM 13 NITs and technology, have you formed an educated opinion
01:37:16PM 14 about how both NITs in general and this NIT worked?

01:37:20PM 15 A. I think I have a pretty good idea of how NITs work,
01:37:24PM 16 in general. And then in both by reading the report that
01:37:26PM 17 Vlad has prepared, and talking and exchanging emails with
01:37:29PM 18 him, I think I have a good idea of what happened here.

01:37:33PM 19 Q. Can you just describe that to the judge, to the best
01:37:35PM 20 of your knowledge?

01:37:35PM 21 A. As I was sort of explaining before, computers are
01:37:40PM 22 programmed to have a certain basic level of cybersecurity.
01:37:45PM 23 They only will allow websites to instruct them to do a
01:37:48PM 24 limited subset of things. The NIT in this case targeted
01:37:52PM 25 people who were using the Tor browser, and so it is

01:37:55PM 1 necessary just for this moment to say that the Tor browser
01:37:59PM 2 is programmed to protect even more information than your
01:38:02PM 3 normal web browser would protect.

01:38:05PM 4 Q. Let's just stop there. So if you have a Tor browser,
01:38:08PM 5 and you are working on the Tor network, it is like you
01:38:10PM 6 have added firewalls or security provisions in your
01:38:14PM 7 computer to protect your privacy; is that correct?

01:38:16PM 8 A. Yes. And not only do you have these additional
01:38:19PM 9 protections, but in fact they slow down your experience.
01:38:22PM 10 So people who are using Tor are experiencing a less rich,
01:38:26PM 11 less fast internet, in exchange for these additional
01:38:30PM 12 protections, which protect their privacy, both information
01:38:33PM 13 about where they are going and information about -- and
01:38:37PM 14 also protecting information about the websites themselves.

01:38:40PM 15 Q. And those protections are on the user's computer; in
01:38:45PM 16 this case it would be Mr. Michaud's computer, correct?

01:38:47PM 17 A. Yes. There is a special web browser that runs within
01:38:51PM 18 the Tor software, and it has been specially configured to
01:38:54PM 19 protect itself from things that websites might try and do
01:38:58PM 20 to force it to reveal identifying information, like an IP
01:39:02PM 21 address.

01:39:02PM 22 Q. When you say "force it to reveal," what is that
01:39:06PM 23 process?

01:39:07PM 24 A. So the Tor software has sort of two separate privacy
01:39:14PM 25 protecting components. The first is the Tor network

01:39:18PM 1 itself. There is a diagram in the book that the
01:39:22PM 2 prosecution provided that sort of shows how things go
01:39:25PM 3 through the Tor network. But, generally, instead of your
01:39:29PM 4 computer contacting the website that you are visiting,
01:39:31PM 5 with Tor your computer bounces the connection through a
01:39:34PM 6 bunch of servers along the way.

01:39:36PM 7 And the purpose of that is to hide the trail. So
01:39:38PM 8 instead of passing a note directly to the judge, I would
01:39:41PM 9 instead pass a note to the lawyer over there, and then the
01:39:45PM 10 lawyer over there would pass the note to someone else in
01:39:46PM 11 the back, and then eventually it would reach you. It gets
01:39:49PM 12 there in the end, but it might take a bit more time to get
01:39:52PM 13 there because of all these people passing it along. That
01:39:54PM 14 is one of the privacy preserving features in Tor, which is
01:39:58PM 15 that it hides the trail through the use of these servers.

01:40:02PM 16 Secondly, the Tor browser -- It is a web browser --
01:40:06PM 17 It is actually a variant of Firefox, which is a very
01:40:08PM 18 popular piece of web browsing software that has been --
19 Q. Slow it down a little.

01:40:13PM 20 A. Sorry. So there is a special customized version of
01:40:17PM 21 the Firefox web browser that has been modified to be even
01:40:22PM 22 more secure.

01:40:23PM 23 Essentially there are tradeoffs on the internet.
01:40:26PM 24 There are some features that make websites more
01:40:29PM 25 interactive, that allow you to have rich media, video,

01:40:32PM 1 sound, an immersive experience. But those futures can
01:40:36PM 2 also be exploited by malicious parties to learn private
01:40:41PM 3 information about you.

01:40:42PM 4 Q. When you say "malicious parties," you don't mean
01:40:45PM 5 their intentions, but you are talking in code sense in
01:40:48PM 6 terms of they are trying to get your computer to do things
01:40:50PM 7 that you would not otherwise do?

01:40:52PM 8 A. I'm sorry. "Malicious" is a term of art in the
01:40:58PM 9 computer security community. When we say "malicious," we
01:41:01PM 10 mean someone that is trying to do something without the
01:41:02PM 11 knowledge or consent of the computer of the person that it
01:41:05PM 12 is being done to.

01:41:07PM 13 And so the Tor browser has been specially modified to
01:41:10PM 14 turn off many features that regular web browsers have
01:41:15PM 15 enabled. And by turning these features off, it reduces
01:41:19PM 16 the number of ways that a website might try and learn
01:41:22PM 17 private information about the person using the Tor
01:41:24PM 18 software.

01:41:25PM 19 Q. When you say it is private, it is information that
01:41:27PM 20 the person, the user, at their computer, is not otherwise
01:41:30PM 21 transmitting or wanting to make public; is that correct?

01:41:33PM 22 A. Well, regular people don't transmit this information
01:41:37PM 23 anyway. This is stuff that is being transmitted by your
01:41:41PM 24 computer without your knowledge or consent to begin with.
01:41:44PM 25 The Tor browser transmits less information to websites

01:41:47PM 1 than a normal website -- than a normal web browser
01:41:51PM 2 transmits.

01:41:52PM 3 And then in addition to that, the Tor browser will
01:41:54PM 4 refuse requests by websites to reveal information that a
01:41:58PM 5 normal web browser would otherwise reveal.

01:42:01PM 6 Q. So that is background. Now, based on your review of
01:42:04PM 7 the discovery, your consultation, Agent Alfin's testimony
01:42:07PM 8 today about the NIT and how it worked, can you just
01:42:10PM 9 explain to the judge -- And really what we want to
01:42:13PM 10 clarify is the locations at which various things happened.
01:42:18PM 11 Can you do that step-by-step from where the NIT is first
01:42:22PM 12 programmed through the capture of data?

01:42:25PM 13 A. I will do the best that I can.

01:42:27PM 14 Q. And go slowly.

01:42:28PM 15 A. Remember, there is one big piece that we don't know
01:42:31PM 16 the answer to, where we don't have some of the code that
01:42:34PM 17 the government hasn't turned over. With the pieces that
01:42:36PM 18 we do have, when someone browses to a website using the
01:42:42PM 19 Tor browser, their computer requests a page. So if you
01:42:47PM 20 are using the Tor browser, your computer asks a website,
01:42:50PM 21 "Please give me this page." That website will then make
01:42:54PM 22 it available and your browser will then go and take it and
01:42:58PM 23 bring it back to your computer.

01:43:01PM 24 In some cases that web page will contain text, and so
01:43:05PM 25 the text will be displayed. In some cases there will be

01:43:08PM 1 images, and the images will be displayed. In some cases
01:43:11PM 2 there is computer programming contained within that
01:43:14PM 3 website, and it will cause your computer to do some action
01:43:17PM 4 before additional text might be displayed.

01:43:20PM 5 Q. When Agent Alfin testified about the NIT running in
01:43:25PM 6 the background, can you just clarify what that means in
01:43:29PM 7 terms of what is being received on the computer in
01:43:32PM 8 Washington?

01:43:33PM 9 A. Sure. From what we understand, from what has become
01:43:40PM 10 public, the web browser -- the Tor web browser in this
01:43:46PM 11 case would have requested information about a particular
01:43:49PM 12 page on this forum, one of these threads.

01:43:52PM 13 Q. So the homepage of this website?

01:43:58PM 14 A. The defendant would have logged in -- is alleged to
01:44:01PM 15 have logged into the homepage, entered a user name and
01:44:05PM 16 password. After that they would have clicked on a link to
01:44:08PM 17 one of these forums. And every time there is a click that
01:44:12PM 18 is happening -- every time someone is clicking on one of
01:44:15PM 19 these links, their browser is requesting new
01:44:18PM 20 information -- a new web page.

01:44:21PM 21 According to what the special agent said, the NIT was
01:44:24PM 22 only delivered after someone went into a thread and then
01:44:27PM 23 clicked on a specific post. So at the point that the
01:44:31PM 24 defendant is accused of clicking on that post, the website
01:44:36PM 25 would have given his Tor browser a web page. Contained

01:44:40PM 1 within that web page would have been an instruction for
01:44:43PM 2 the Tor browser -- not for the defendant, but for the Tor
01:44:47PM 3 browser.

01:44:47PM 4 Q. Let's stop there. When you say "contained," can you
01:44:50PM 5 see that on the web page?

01:44:52PM 6 A. Can a human see it?

01:44:54PM 7 Q. Would the user who is looking for, say, a picture on
01:44:58PM 8 the internet, would they see those instructions?

01:45:01PM 9 A. No, there wouldn't have been any instructions visible
01:45:03PM 10 to a regular user. A high-tech sophisticated person might
01:45:08PM 11 be able to figure that out, but a regular person just
01:45:11PM 12 clicking around is not going to know there has been this
01:45:14PM 13 new special code added to the web page.

01:45:17PM 14 Q. So it is hidden code running in the background. When
01:45:20PM 15 you say "sending instructions," it is not instructions to
01:45:22PM 16 the user, in this case allegedly Mr. Michaud, it is
01:45:26PM 17 instructions to the target computer?

01:45:28PM 18 A. I want to pause on that word "running." The code
01:45:31PM 19 does not run on the website. The code always runs on your
01:45:36PM 20 web browser. So the website tells the web browser, "Do
01:45:39PM 21 this." The code is downloaded to the web browser, the Tor
01:45:42PM 22 browser in this case, in this case in the state of
01:45:45PM 23 Washington. And it is only when the instructions are
01:45:47PM 24 received by the Tor browser here in the state of
01:45:50PM 25 Washington that they are run on that computer, and then do

01:45:54PM 1 whatever the NIT is supposed to do.

01:45:56PM 2 Q. And in this case, from the testimony you have heard,
01:45:58PM 3 what exactly was the NIT supposed to do when it was
01:46:01PM 4 inserted into the Washington computer?

01:46:04PM 5 A. Okay. So this is where it gets a little bit
01:46:08PM 6 complicated.

01:46:09PM 7 Q. Go slowly.

01:46:10PM 8 A. We don't know one of the important bits of
01:46:14PM 9 information. The Tor browser is not supposed to give up
01:46:18PM 10 its real IP address to anyone. That is the one reason
01:46:21PM 11 that you use Tor.

01:46:22PM 12 Q. And that Tor browser -- That is a program that is
01:46:25PM 13 running on the Washington computer?

01:46:26PM 14 A. On the computer of the defendant. The Tor browser
01:46:30PM 15 would have been running there. The one thing the Tor is
01:46:32PM 16 not supposed to do is give up your IP address. And if a
01:46:36PM 17 website that you are visiting with a Tor browser asks for
01:46:38PM 18 your IP address, the Tor browser will say no.

01:46:42PM 19 If you think -- I know you have said think of the Tor
01:46:45PM 20 browser like a firewall. Think of it more like a guard
01:46:48PM 21 dog, a guard dog around a house. If the guard dog is
01:46:51PM 22 trained to bark at every person who approaches the house,
01:46:55PM 23 and someone approaches and the guard dog doesn't bark,
01:46:59PM 24 well, you have to ask, what happened? Why didn't the
01:47:02PM 25 guard dog bark? So something mysterious happened in this

01:47:07PM 1 case that caused the Tor browser to even let the NIT do
01:47:10PM 2 what it wanted to do, which was to collect this
01:47:13PM 3 information that the Tor browser would never ordinarily
01:47:16PM 4 give up.

01:47:16PM 5 Q. So we don't know exactly the process because we don't
01:47:19PM 6 have all the code. But just to clarify, the NIT is hidden
01:47:23PM 7 code that is sent to the computer in Washington, correct?

01:47:26PM 8 A. It is hidden code that is sent to the computer in
01:47:29PM 9 Washington State that somehow causes the computer in
01:47:31PM 10 Washington state to do something that it would not
01:47:35PM 11 normally do.

01:47:35PM 12 Q. So not only is the NIT going to Washington State, it
01:47:39PM 13 is now giving instructions or overriding instructions on
01:47:43PM 14 that Washington computer?

01:47:46PM 15 A. Yes. If you want to use the guard dog analogy, you
01:47:49PM 16 could think of it as maybe putting a sleeping pill in the
01:47:52PM 17 dog food.

01:47:53PM 18 Q. Now, once those override instructions are executed on
01:47:58PM 19 the Washington computer after this delivery, I guess from
01:48:02PM 20 Virginia, what is the next step in what the NIT, from all
01:48:05PM 21 of your research and review of discovery, did?

01:48:08PM 22 A. So once the NIT had bypassed the security controls
01:48:12PM 23 within the Tor browser, it then had to collect information
01:48:16PM 24 from the computer that it wished to send back. In this
01:48:19PM 25 case it would be the IP address, which is an address that

01:48:22PM 1 links the computer to a residential internet account. It
01:48:25PM 2 would be what is called the MAC address, which is a unique
01:48:29PM 3 serial number associated with your wi-fi card, programmed
01:48:33PM 4 in the factory of the wi-fi card manufacturer. There
01:48:37PM 5 would be some other information about the operating system
01:48:39PM 6 that the special agent read out when he was on the stand,
01:48:43PM 7 the user name on the computer, which version of Windows
01:48:46PM 8 you are running, some basic information.

01:48:49PM 9 But to learn that information, before the NIT could
01:48:51PM 10 transmit that information back to the computer in
01:48:54PM 11 Virginia, it would first have to go and collect it. So if
01:48:58PM 12 you think of this as information that is in a house, well,
01:49:00PM 13 maybe one piece of it is in the bedroom, and another piece
01:49:04PM 14 is in the living room, one piece of it is in the drawer.
01:49:06PM 15 The NIT first has to go and collect the information from
01:49:09PM 16 different parts of the computer. And then once it has
01:49:13PM 17 that information, then it would transmit it back to the
01:49:16PM 18 server in Virginia.

01:49:18PM 19 Q. So if I understand the process, the NIT bypasses
01:49:24PM 20 security or overrides security features on the Washington
01:49:27PM 21 computer. First step, right? And then second, it
01:49:30PM 22 actually collects data or evidence on that computer. And
01:49:34PM 23 then the third step, after it has seized the Washington
01:49:37PM 24 data in this case, it then wraps it up in like a little
01:49:42PM 25 evidence bag and delivers it to the FBI in Virginia?

01:49:45PM 1 A. That sounds right. Although I'm not sure about the
01:49:49PM 2 evidence bag. It transmits it back to the computer in
01:49:52PM 3 Virginia.

01:49:52PM 4 Q. And then once that data has been transmitted back, it
01:49:57PM 5 is stored, apparently, on an FBI server; is that correct?

01:50:01PM 6 A. The special agent said that the server is under the
01:50:06PM 7 government's control. I am not sure how much I can say in
01:50:10PM 8 this room about where we think the server is or which
01:50:13PM 9 company we think might have been running the server.

01:50:15PM 10 Q. I don't want you to --

01:50:17PM 11 A. A computer in Virginia.

01:50:20PM 12 Q. Is it then fair to say after this search and seizure
01:50:24PM 13 in Washington, then really what is going on is it is in
01:50:26PM 14 like an evidence room in Virginia where they keep that
01:50:28PM 15 evidence until they need it?

01:50:31PM 16 MR. BECKER: Object to leading at this point, your
01:50:33PM 17 Honor. I think we are just reiterating testimony.

01:50:34PM 18 THE COURT: That is a fair objection.

01:50:36PM 19 By Mr. Fieman:

01:50:36PM 20 Q. Describe then what the storage in Virginia is about.

01:50:38PM 21 A. Once the data has been transmitted by the NIT, I have
01:50:43PM 22 no idea what the government would do with it. We know
01:50:46PM 23 that it was transmitted to a computer in Virginia. At
01:50:49PM 24 that point we have no -- They haven't turned over
01:50:51PM 25 information about how it is stored, or who has access to

01:50:54PM 1 it, or whether it is printed on paper or stored live in a
01:50:58PM 2 computer. We don't know how it is maintained.

01:51:01PM 3 Q. Now, you had just briefly mentioned that there are
01:51:08PM 4 parts of the code that are missing data, and so you have
01:51:12PM 5 to be a little reserved about your opinions, correct?

01:51:14PM 6 A. I do not know how the NIT was able to get the Tor
01:51:21PM 7 browser to do this thing that the Tor browser would never
01:51:25PM 8 normally do. The general way that one does this -- the
01:51:29PM 9 general way of describing this is to exploit security
01:51:35PM 10 flaws in software.

01:51:36PM 11 In fact, when I started testifying here I used the
01:51:39PM 12 term "malware." And in the computer security community
01:51:44PM 13 the term "malware" really describes software that is doing
01:51:48PM 14 things that the person whose computer it is running on
01:51:54PM 15 doesn't know it is doing or doesn't want it to do. In
01:51:58PM 16 many, many cases malware, to effectively function, first
01:52:01PM 17 must exploit some security flaw in the software that is
01:52:05PM 18 running on your computer, whether that is your web
01:52:07PM 19 browser, a piece of email software, or PowerPoint, or
01:52:11PM 20 Microsoft Word.

01:52:12PM 21 All of these programs that we run on our computer, the
01:52:15PM 22 engineers who write them do the best job they can, but
01:52:19PM 23 sometimes they make mistakes. There are a lot of people
01:52:21PM 24 out there that are looking to find these flaws. If you
01:52:24PM 25 can find one of these flaws, you can write special code

01:52:27PM 1 that takes advantage of the flaw, and then lets you run
01:52:30PM 2 code on a computer that the computer probably shouldn't
01:52:33PM 3 run normally, or obtain information that you wouldn't
01:52:36PM 4 normally be able to get.

01:52:37PM 5 Q. And you say not normally be able to get. Let me ask
01:52:41PM 6 you this: Based on all your review of the discovery and
01:52:44PM 7 the testimony, if the NIT had not been delivered to the
01:52:47PM 8 Washington computer, and collected the data for the
01:52:51PM 9 Washington computer, would the website otherwise have the
01:52:56PM 10 IP address and other identifying data in the normal course
01:52:59PM 11 of events?

01:53:00PM 12 A. No. The Tor browser is programmed to protect those
01:53:03PM 13 pieces of information.

01:53:11PM 14 MR. FIEMAN: Your Honor, I just have one other
01:53:13PM 15 brief area and then I will be able to wrap up.

01:53:14PM 16 By Mr. Fieman:

01:53:14PM 17 Q. From a technical standpoint, I want to ask you about
01:53:17PM 18 when the NIT was sent to Washington, how it was deployed.
01:53:20PM 19 You have reviewed the warrant application in this case --
01:53:24PM 20 the NIT warrant application?

01:53:26PM 21 A. Yes, sir.

01:53:26PM 22 Q. You are aware the warrant application, I think,
01:53:29PM 23 allowed for the FBI to deploy -- to send the NIT
01:53:35PM 24 anywhere at the time people logged into the homepage; is
01:53:37PM 25 that correct?

01:53:37PM 1 A. I am aware of what the warrant authorized, as far as
01:53:41PM 2 one can be aware as a non-lawyer.

01:53:43PM 3 Q. As of that point, the NIT could be deployed and
01:53:48PM 4 collect all this information from anywhere in the world,
01:53:50PM 5 correct?

01:53:50PM 6 A. At the time that the NIT is delivered to the
01:53:56PM 7 computer, the government doesn't know where the computers
01:53:58PM 8 are. The computer could be in the state of Washington, it
01:54:01PM 9 could be in Utah, it could also be in France or Spain.
01:54:05PM 10 Again, the Tor network is a global network with hundreds
01:54:09PM 11 of thousands of users located around the world. There is
01:54:13PM 12 no way of knowing ahead of time where any one of those
01:54:16PM 13 users of Tor might be.

01:54:18PM 14 Q. Now, just from a technical standpoint, if the NIT
01:54:21PM 15 could be deployed at the homepage, was there any technical
01:54:26PM 16 reason that you are aware of why the website would have to
01:54:31PM 17 retain, and publish, and distribute child pornography
01:54:37PM 18 inside the website in order to accomplish the NIT
01:54:40PM 19 deployment?

01:54:40PM 20 MR. BECKER: Objection, your Honor. You have
01:54:42PM 21 already ruled on this issue. This is not relevant to any
01:54:45PM 22 of the suppression issues here.

01:54:49PM 23 MR. FIEMAN: Your Honor, I just want to talk about
01:54:50PM 24 the point of deployment, and that the point of deployment
01:54:54PM 25 could have occurred from the homepage in all cases.

01:54:56PM 1 THE COURT: I'm not sure I understand the question
01:54:59PM 2 here.

01:55:00PM 3 By Mr. Fieman:

01:55:00PM 4 Q. Is there any reason why all of the NITs, in order to
01:55:03PM 5 collect IP addresses pursuant to this warrant, could not
01:55:06PM 6 have been deployed simply from the homepage, that you are
01:55:10PM 7 aware of?

01:55:11PM 8 A. You can deliver a NIT from any web page on that site.
01:55:17PM 9 The fact that the government chose to deliver it on a few
01:55:22PM 10 select pages after people logged in or after people had
01:55:24PM 11 clicked a few links, that seems, from a technical
01:55:26PM 12 standpoint, arbitrary. They could have even put it on the
01:55:28PM 13 homepage before people logged in or after people logged
01:55:42PM 14 in.

01:55:46PM 15 Q. Slow down. That's okay. You are an east coaster
01:55:51PM 16 like me, Dr. Soghoian. Is there any point in sort of the
01:55:58PM 17 physical process of the NIT search that you believe we
01:56:02PM 18 have not covered that the court should be aware of?

01:56:06PM 19 A. I am just thinking. For the issues that you guys
01:56:21PM 20 have been litigating today, no.

01:56:26PM 21 MR. FIEMAN: Your Honor, do you have any questions
01:56:27PM 22 that we have not addressed at this point?

01:56:29PM 23 THE COURT: No. Go ahead.

01:56:31PM 24 MR. FIEMAN: Thank you, your Honor.

01:56:35PM 25 CROSS-EXAMINATION

01:56:38PM 1 By Mr. Becker:

01:56:45PM 2 Q. Good afternoon, Dr. Soghoian.

01:56:47PM 3 A. Hi.

01:56:48PM 4 Q. Would you agree that the Tor Project does not
01:56:56PM 5 guarantee perfect anonymity to its users?

01:56:59PM 6 A. My understanding is that the homepage of the Tor
01:57:02PM 7 Project tells people that it cannot deliver perfect
01:57:05PM 8 security.

01:57:05PM 9 Q. Right from the homepage of the Tor Project it advises
01:57:08PM 10 its users that it cannot deliver, as you said, perfect
01:57:11PM 11 security; is that correct?

01:57:12PM 12 A. What I will say, though, is that the Tor Project is
01:57:16PM 13 about ten years old. It has received millions of dollars
01:57:20PM 14 of grants. It is the best thing that the computer
01:57:22PM 15 security research community has come up with thus far.

01:57:25PM 16 Q. It has some great uses, is that fair to say?

01:57:28PM 17 A. The Tor Project is being used by Facebook, it is
01:57:33PM 18 being used by newspapers, ProPublica, and many newspapers
01:57:38PM 19 that now run whistle blowing websites. As I'm sure you
01:57:41PM 20 know, the Tor Project was originally -- the technology was
01:57:44PM 21 created by the U.S. Navy, the Naval Research Lab, and the
01:57:47PM 22 U.S. government has been and continues to be the biggest
01:57:51PM 23 funder of Tor.

01:57:51PM 24 Q. As we said, it can be used for many laudable,
01:57:55PM 25 positive purposes, correct?

01:57:56PM 1 A. That is correct. And my understanding is it is also
01:58:00PM 2 used by many law enforcement agencies so that they can
01:58:03PM 3 conduct covert investigations online.

01:58:05PM 4 Q. Do you agree it can also be misused for illicit
01:58:09PM 5 purposes?

01:58:09PM 6 A. That is a complicated question.

01:58:11PM 7 Q. Is it?

01:58:12PM 8 A. Yes. Because the original creators of Tor -- When
01:58:16PM 9 the Navy created Tor, the purpose was to allow naval
01:58:20PM 10 investigators to research people online so that they could
01:58:23PM 11 investigate whatever crimes the Navy is researching
01:58:26PM 12 without tipping off the world with the fact that the Navy
01:58:30PM 13 is researching them. Now, if you have this technology
01:58:32PM 14 that is protecting the privacy of naval investigators, and
01:58:35PM 15 the only people who are using it are naval investigators,
01:58:38PM 16 well, then you are not anonymous.

01:58:40PM 17 Q. Are they the only people using Tor?

01:58:42PM 18 A. No.

01:58:42PM 19 Q. Would you agree that criminals use Tor?

01:58:45PM 20 A. That is by design.

01:58:46PM 21 Q. Criminals use Tor by design?

01:58:49PM 22 A. When the Navy created Tor, and put the technology out
01:58:52PM 23 there, they knew that they would have both good and bad
01:58:55PM 24 users. If you only have one --

01:58:57PM 25 Q. So you agree there are good --

01:58:59PM 1 MR. FIEMAN: Your Honor, if Dr. Soghoian could
01:59:01PM 2 finish his answer.

01:59:02PM 3 THE COURT: You interrupted the witness.

01:59:05PM 4 THE WITNESS: If you only have naval investigators
01:59:08PM 5 using Tor, then the moment a website receives someone
01:59:11PM 6 coming from Tor -- receives a request from someone using
01:59:15PM 7 Tor, they know that it is the U.S. government. So the
01:59:19PM 8 creators of Tor have a phrase they use, and they use it in
01:59:23PM 9 research papers and elsewhere, it is that anonymity loves
01:59:27PM 10 company. If you want to have a technology that lets
01:59:30PM 11 people blend into the crowd, you need a crowd. And so the
01:59:33PM 12 creators of Tor from day one knew that there would be uses
01:59:38PM 13 of Tor that society would love and uses of Tor that
01:59:42PM 14 society would not love as much.

01:59:44PM 15 By Mr. Becker:

01:59:46PM 16 Q. Let's back around to my question. We agree you can
01:59:50PM 17 use Tor to mask your identity while committing crimes,
01:59:53PM 18 correct?

01:59:54PM 19 A. You can use Tor to mask your identity when you are
01:59:58PM 20 online, and people can commit crimes online.

02:00:00PM 21 Q. You can use Tor to mask your identity while you
02:00:03PM 22 commit crimes online through Tor?

02:00:07PM 23 A. Tor is a communication technology. That is like
02:00:11PM 24 saying, can you use a car to commit a crime? Well, yeah,
02:00:14PM 25 I guess so. But it is a regular technology that has good

02:00:17PM 1 users and bad users. That doesn't mean the technology has
02:00:21PM 2 some kind of morality associated with it. It is like
02:00:25PM 3 FedEx, or the post office, or the telephone line, it is a
02:00:29PM 4 core communications and transportation technology.

02:00:31PM 5 Q. Sure. And I'm sure we would agree that no matter
02:00:34PM 6 what sort of communication technology that criminals are
02:00:38PM 7 using, law enforcement needs to take action based on
02:00:41PM 8 whatever that technology is; is that fair to say?

02:00:43PM 9 A. I think if law enforcement is concerned about people
02:00:47PM 10 using Tor -- about criminals using Tor, I think the most
02:00:51PM 11 rational approach would be to stop the U.S. government
02:00:54PM 12 from funding Tor.

02:00:55PM 13 Q. You don't want criminals who are using Tor to be
02:00:58PM 14 investigated?

02:00:58PM 15 A. No, I am not saying that. I am saying if you don't
02:01:01PM 16 want criminals to hide their identity using Tor, then the
02:01:05PM 17 U.S. government should stop writing the checks that are
02:01:09PM 18 paying for Tor to be developed. If you are worried about
02:01:11PM 19 the availability of a technology that lets people hide,
02:01:14PM 20 and you don't think -- you think it is being misused, why
02:01:17PM 21 are you paying for it? Just cut it off.

02:01:23PM 22 Q. Let me ask you some questions about a different area.
02:01:26PM 23 You haven't reviewed any computers or digital evidence
02:01:28PM 24 related to this case; is that right?

02:01:29PM 25 A. No, sir.

02:01:30PM 1 Q. You haven't reviewed any of the computers that were
02:01:33PM 2 seized from the defendant's home?

02:01:34PM 3 A. No, sir.

02:01:34PM 4 Q. You haven't reviewed any computer code that has been
02:01:38PM 5 provided in discovery, correct?

02:01:39PM 6 A. So Vlad, who is our other expert, he has reviewed
02:01:44PM 7 computer code provided to him by DOJ. I have read the
02:01:48PM 8 report that Vlad sent to me, but I have not personally
02:01:52PM 9 reviewed the NIT code.

02:01:55PM 10 MR. BECKER: Your Honor, I would make a Jencks
02:01:57PM 11 request for that report, if we don't have it.

02:01:59PM 12 MR. FIEMAN: I actually don't either, your Honor.
02:02:01PM 13 I was unaware of any written report from Mr. Cirkovic. I
02:02:12PM 14 am not sure there is one at this point. Although, there
02:02:14PM 15 has been, obviously, a lot of conversations with the
02:02:15PM 16 various experts on all sides. So I don't have a report to
02:02:21PM 17 turn over. I will make inquiries, your Honor, absolutely.
02:02:22PM 18 By Mr. Becker:

02:02:23PM 19 Q. Dr. Soghoian, can you describe the written
02:02:25PM 20 communications you have had with the defense expert about
02:02:26PM 21 the analysis of the code?

02:02:28PM 22 A. Sure. He sent me a few-paragraph email describing
02:02:31PM 23 his initial analysis of the shell code.

02:02:34PM 24 Q. Did you sign a protective order before you received
02:02:37PM 25 that?

02:02:37PM 1 A. I agreed to a protective order when I first got
02:02:42PM 2 retained. Whether I signed something, I don't remember.
02:02:47PM 3 I am pretty sure I did. The public defender definitely
02:02:51PM 4 sent me the protective order and asked me to agree to it.
02:02:54PM 5 I would have to consult my records to see if I signed
02:02:57PM 6 something and sent it back.

02:02:58PM 7 MR. BECKER: Your Honor, I would request -- The
02:03:01PM 8 witness has testified about a particular written
02:03:03PM 9 communication during the course of this proceeding. I
02:03:06PM 10 would request that and other communications.

02:03:11PM 11 MR. FIEMAN: No objection, your Honor.

02:03:13PM 12 THE WITNESS: Is there any way I can ask for a
02:03:15PM 13 glass of water? Is that possible?

02:03:46PM 14 By Mr. Becker:

02:03:48PM 15 Q. Doctor, just a basic point. In terms of
02:03:50PM 16 communications on Tor, it is correct that when a user
02:03:54PM 17 communicates through Tor, the user is still using IP
02:03:58PM 18 addresses in order to communicate, correct?

02:04:02PM 19 A. Someone doesn't use an IP address to communicate.

02:04:05PM 20 Q. IP addresses route communications, even through Tor?

02:04:08PM 21 A. No, an IP address is a number assigned to you. You
02:04:12PM 22 use the internet, and in particular the IP protocol, to
02:04:16PM 23 communicate. But you don't use your address. It is not
02:04:19PM 24 like -- When you write a letter to someone, you don't use
02:04:21PM 25 your physical address to communicate, you use the post

02:04:24PM 1 office to communicate, and your address is printed in the
02:04:26PM 2 top left-hand corner of the letter.

02:04:28PM 3 Q. Very well. Does Tor not use IP addresses? Would
02:04:32PM 4 that be a fair statement?

02:04:33PM 5 A. Tor is what is called an overlay network. So there
02:04:37PM 6 is a network on top of the internet.

02:04:43PM 7 Q. Would it be correct to say using Tor means you are
02:04:46PM 8 not using IP addresses to communicate?

02:04:48PM 9 A. Again, as I said before, you don't use an IP address
02:04:51PM 10 to communicate. You have an IP address. You use the IP
02:04:55PM 11 protocol to communicate. I am sorry if it sounds like I
02:04:59PM 12 am lost on these details, but you don't use an IP address
02:05:05PM 13 to communicate.

02:05:06PM 14 Q. You used and defined the term earlier that you called
02:05:12PM 15 "malicious." You defined that as someone who -- an entity
02:05:17PM 16 that was sending something or using something without
02:05:21PM 17 knowledge or consent; is that fair?

02:05:24PM 18 A. I'm sorry. Can you ask that question again, please?

02:05:26PM 19 Q. Sure. You were defining a term earlier as
02:05:29PM 20 "malicious." You said in your community you define that
02:05:33PM 21 as something happening without knowledge or consent?

02:05:35PM 22 A. That is a component of malware, yes, sir.

02:05:40PM 23 Q. Would it be possible for that communication to be
02:05:44PM 24 authorized and for you to still describe it as malicious?

02:05:49PM 25 A. So the question is, can something be authorized and

02:05:51PM 1 still malicious?

02:05:53PM 2 Q. Yeah.

02:05:54PM 3 A. Authorized by whom?

02:05:56PM 4 Q. A court.

02:05:59PM 5 A. I think in the computer security community malware is
02:06:05PM 6 really about -- the definition of malware depends on the
02:06:08PM 7 knowledge of the user and the consent of the user.

02:06:11PM 8 Q. So you don't think the courts have the ability to --

02:06:21PM 9 MR. BECKER: I will withdraw that. No further
02:06:22PM 10 questions, your Honor.

02:06:24PM 11 MR. FIEMAN: Very briefly, your Honor.

02:06:27PM 12 REDIRECT EXAMINATION

02:06:30PM 13 By Mr. Fieman:

02:06:31PM 14 Q. Mr. Becker started with a very simple question. He
02:06:33PM 15 asked you whether Tor -- Tor does not promise to deliver
02:06:36PM 16 perfect security. Do you recall that?

02:06:38PM 17 A. I do recall that exchange.

02:06:39PM 18 Q. Is it also fair to say that a burglar alarm or a home
02:06:43PM 19 alarm does not deliver perfect security?

02:06:45PM 20 A. That is correct, and neither does the lock on my
02:06:48PM 21 front door.

02:06:48PM 22 Q. But the fact that it doesn't deliver perfect
02:06:51PM 23 security, does that make it okay for somebody to break the
02:06:54PM 24 lock on your front door and go in and take information
02:06:56PM 25 from your home?

02:06:57PM 1 A. I am not sure if that is the right question for me.

02:07:01PM 2 I will say --

02:07:01PM 3 Q. Just as a matter of common sense.

02:07:03PM 4 A. As an individual, no, it doesn't make it okay.

02:07:08PM 5 MR. FIEMAN: Thank you. No further questions.

02:07:15PM 6 THE COURT: It sort of sounds like no one should
02:07:19PM 7 expect privacy with whatever is on their computer and on
02:07:25PM 8 the internet?

02:07:26PM 9 THE WITNESS: It is very hard for individuals to
02:07:28PM 10 protect their privacy online. It is for that reason that
02:07:35PM 11 the government has spent so much money trying to create
02:07:39PM 12 technologies that let people protect their privacy. It is
02:07:43PM 13 really hard for the average person to protect their
02:07:45PM 14 privacy online. Those of us who are trying to protect our
02:07:48PM 15 privacy, we have to work hard. Sometimes we get a slower
02:07:52PM 16 internet experience. Sometimes we have to use software
02:07:57PM 17 that is not as easy to use in order to protect our
02:08:00PM 18 privacy.

02:08:00PM 19 There is a huge amount of research that is going on in
02:08:03PM 20 this space to create tools that let the average person
02:08:06PM 21 protect themselves. I have spent much of the last few
02:08:11PM 22 years trying to help the legal community to protect their
02:08:13PM 23 privacy, trying to get law firms and the courts to employ
02:08:17PM 24 basic privacy and security technology to protect what you
02:08:21PM 25 all are doing. It is hard for the average person when

02:08:24PM 1 this stuff is so high-tech. My hope is over the next few
02:08:27PM 2 years we will get better and easier technology that will
02:08:31PM 3 protect people.

02:08:34PM 4 THE COURT: We started this -- or in the middle of
02:08:39PM 5 it, I guess, we came to the Tor instructions, or whatever,
02:08:45PM 6 that say that it does not deliver perfect security. Is
02:08:49PM 7 there any perfect security at this point, other than not
02:08:55PM 8 putting it in there?

02:08:57PM 9 THE WITNESS: In my community, and in the computer
02:09:00PM 10 security community, we use concepts like defense in depth.

02:09:03PM 11 THE COURT: What?

02:09:04PM 12 THE WITNESS: Defense in depth. So rather than
02:09:08PM 13 having one wall protecting your castle, you have ten
02:09:12PM 14 walls. That way if the barbarians get over the first
02:09:15PM 15 wall, they still have nine more they have to overcome.

02:09:18PM 16 THE COURT: That is kind of what Tor does?

02:09:21PM 17 THE WITNESS: The Tor has at least two walls.
02:09:23PM 18 Probably over the next few years they are going to add
02:09:25PM 19 some more. I was having lunch with a DHS official this
02:09:32PM 20 week -- a Department of Homeland Security official, about
02:09:34PM 21 the technology they are funding to help create even more
02:09:37PM 22 walls. When you look at some of the data breaches that
02:09:41PM 23 have happened in the last few years, the OPM breach, where
02:09:45PM 24 all these federal employees had their private information
02:09:48PM 25 lost and stolen by China, it is really hard to design

02:09:51PM 1 secure software and to protect data.

02:09:54PM 2 The old approach was let's keep the bad guys out. Now
02:09:58PM 3 the approach is, how do we stop the bad guys before they
02:10:01PM 4 get all the way to the inner room of the house, or how do
02:10:05PM 5 we limit their access to information. There is an arms
02:10:11PM 6 race going on right now between those who are trying to
02:10:13PM 7 protect data and those who are trying to exploit data.
02:10:17PM 8 This is a really interesting time. The unfortunate thing
02:10:20PM 9 is for regular people it is really hard to protect
02:10:23PM 10 yourself online.

02:10:25PM 11 THE COURT: Okay. Thank you.

02:10:28PM 12 THE WITNESS: Thank you, sir.

02:10:33PM 13 THE COURT: Any other evidence to be offered here?

02:10:35PM 14 MR. FIEMAN: No other evidence, your Honor, from
02:10:37PM 15 the defense.

02:10:47PM 16 THE COURT: Let me figure here a little bit. In a
02:11:17PM 17 practical sense, you have about a half hour apiece to
02:11:20PM 18 argue this, which should be enough. When you get to the
02:11:24PM 19 U.S. Supreme Court they won't give you that much time.

02:11:29PM 20 MR. FIEMAN: Who would you like to hear from
02:11:31PM 21 first?

02:11:31PM 22 THE COURT: Well, it is your motion, or motions.

02:11:39PM 23 MR. FIEMAN: Your Honor, I think we are down to
02:11:41PM 24 essentially the core issue around which everything else
02:11:45PM 25 revolves. And it is really a brick and mortar issue. We

02:11:53PM 1 have resolved it. This search happened on a computer
02:11:59PM 2 located in Vancouver, Washington. The warrant on its face
02:12:07PM 3 is limited to persons and property in the Eastern District
02:12:11PM 4 of Virginia.

02:12:12PM 5 The first question that you asked us to respond to,
02:12:18PM 6 your Honor, when you issued your order on Wednesday was,
02:12:22PM 7 where did this search happen? We gave you a written
02:12:28PM 8 response citing the government's own stipulations in other
02:12:35PM 9 NIT cases, and its own pleadings. This was a Washington
02:12:40PM 10 search.

02:12:42PM 11 Now, in and of itself, is that unconstitutional, or a
02:12:46PM 12 bad thing? No. But the problem that the government is
02:12:50PM 13 confronting is severalfold.

02:12:52PM 14 One is, as we cited, they obtained a warrant in
02:12:56PM 15 Virginia that on its face is limited to Virginia. And it
02:13:00PM 16 is a simple, straightforward rule. We cited Sedaghaty,
02:13:06PM 17 and all the other cases, that say if the search exceeds
02:13:12PM 18 the scope, the authorization occurs at a location that is
02:13:15PM 19 not authorized, suppression is automatic. There is no
02:13:19PM 20 good-faith issues, there are no Franks issues.

02:13:22PM 21 So the question is then, why did the government submit
02:13:27PM 22 a warrant to the magistrate judge in Virginia which on its
02:13:33PM 23 face informed Judge Buchanan that this is an Eastern
02:13:37PM 24 District of Virginia search, when previously they had at
02:13:42PM 25 least indicated in the Cottom case and the other, that the

02:13:46PM 1 searches occurred both in the district and elsewhere?

02:13:51PM 2 I respectfully submit to your Honor that you have seen
02:13:57PM 3 in the course of these several hours of proceedings
02:14:00PM 4 exactly why they did that. Because after Judge Smith's
02:14:05PM 5 decision in In Re Warrant, and looking at the plain
02:14:09PM 6 language of Rule 41, which they are in the process of
02:14:14PM 7 trying to get changed, because it does not allow for this,
02:14:20PM 8 they obtained authorization. No matter whether it was
02:14:24PM 9 well intentioned, whether they disclosed everything, that
02:14:26PM 10 warrant says Eastern District of Virginia.

02:14:29PM 11 And Mr. Michaud's data was not only seized here in
02:14:35PM 12 Washington, but they in fact had to bypass security
02:14:39PM 13 measures, like the house alarms, on his computer in
02:14:42PM 14 Washington, look through the data on his computer in order
02:14:46PM 15 to get the identifying information that they sought, and
02:14:49PM 16 then took it back to the evidence room in Virginia.

02:14:54PM 17 In their own pleadings that we have shown to you, they
02:14:58PM 18 always refer to this as information seized from
02:15:00PM 19 Mr. Michaud's computer. So all of this about the
02:15:03PM 20 target -- the target being the server in Washington, that
02:15:07PM 21 they are going to retrieve the data from there, the whole
02:15:09PM 22 point of this is they couldn't get that information in
02:15:12PM 23 Virginia. They had to go everywhere else to target
02:15:16PM 24 computers to get it. Your Honor, that is, first of all,
02:15:19PM 25 unfortunately for them, still not allowed by Rule 41.

02:15:24PM 1 More importantly, what has been driving my sense of
02:15:26PM 2 frustration with this case, if you want to do that, make
02:15:32PM 3 it clear to the judge that you are trying to do that.

02:15:35PM 4 I honestly believe that Judge Buchanan, when she
02:15:38PM 5 looked at this warrant, because it is what I interpreted
02:15:41PM 6 the warrant to mean when I first read it, that they were
02:15:45PM 7 going to search any number of computers in the Eastern
02:15:47PM 8 District of Virginia that might be logging into this site.
02:15:50PM 9 But you will not find anything that tells the judge this
02:15:53PM 10 is a worldwide warrant. If you look at the face of the
02:15:56PM 11 warrant itself, it says Eastern District of Virginia,
02:15:59PM 12 stop, period, nothing more. So for those defendants who
02:16:04PM 13 are in Virginia that have been caught up in this case,
02:16:07PM 14 they may have to raise different issues.

02:16:12PM 15 And that's why I have been hitting at the duty of
02:16:15PM 16 candor. Your Honor, it may be that this needs to work its
02:16:20PM 17 way through the courts. It may be that the judges, in
02:16:23PM 18 amending the rule -- the Supreme Court amending the rule,
02:16:25PM 19 if eventually that's what it does, because that is what
02:16:28PM 20 the Department of Justice is hoping for, then the law will
02:16:31PM 21 change.

02:16:31PM 22 But as long as the law stands, the government needs to
02:16:33PM 23 tell the judges exactly what kind of authorization they
02:16:37PM 24 are seeking. And not in the words of their own head of
02:16:42PM 25 operations and technology, Amy Hess, as we cited, not

02:16:46PM 1 leaving it for the judges to try and figure out what is
02:16:49PM 2 going on, hoping against hope they won't ask the follow-up
02:16:53PM 3 questions, but to make it plain. And that is exactly what
02:16:58PM 4 Judge Kozinski said in the CDT decisions, a duty of
02:17:06PM 5 candor.

02:17:06PM 6 Now, your Honor, I just ask you, in terms of the
02:17:09PM 7 dispositive issue, to look at the four corners of the
02:17:12PM 8 warrant, what is printed on the face, and after all of
02:17:16PM 9 this testimony and the government's pleadings, which we
02:17:19PM 10 would direct you to, it is a Washington search on an
02:17:22PM 11 Eastern District of Virginia warrant. It sounds like a
02:17:27PM 12 very simple way to decide a very complex issue, but
02:17:30PM 13 everything else feeds into that.

02:17:36PM 14 Why did they draft it that way? Now let's move
02:17:40PM 15 forward. Because Rule 41 doesn't allow it. And they have
02:17:44PM 16 never said or claimed that Rule 41 does not apply. There
02:17:48PM 17 is no exemptions to Rule 41. Rule 41 is codified in
02:17:54PM 18 18 U.S. 3103. It is the law. Sometimes we don't agree
02:18:00PM 19 with it. Sometimes if you are the government you wish it
02:18:03PM 20 was more expansive, but it is the law.

02:18:07PM 21 And regardless of the fact that they clearly and
02:18:12PM 22 deliberately violated Rule 41, and their explanations
02:18:17PM 23 about how Rule 41 might apply would not pass muster in a
02:18:23PM 24 1L class, the upshot is still that the warrant itself says
02:18:28PM 25 the Eastern District of Virginia, full stop.

02:18:33PM 1 And Judge Smith in his In Re warrant opinion got it
02:18:38PM 2 right. We may be talking about technology in cyberspace,
02:18:43PM 3 and data, but it is not just a cloud. They have a
02:18:48PM 4 physical location for these searches. And all the
02:18:52PM 5 testimony and the government's pleadings establishes the
02:18:54PM 6 physical location of that data search and extraction
02:18:57PM 7 occurred in Washington State.

02:19:04PM 8 Now, your Honor, I have indicated under Sedaghaty and
02:19:07PM 9 the other cases the fact that the warrant was executed in
02:19:10PM 10 Washington with a -- excuse me, that the search was
02:19:13PM 11 executed in Washington with an Eastern District warrant
02:19:16PM 12 requires suppression. But I am also going to say that the
02:19:20PM 13 Rule 41 violations require suppression also. Because in
02:19:24PM 14 all of the pleadings that have come from the government,
02:19:26PM 15 not once have they talked about Weiland, which is the case
02:19:29PM 16 that we cited, which says that suppression is required for
02:19:32PM 17 a Rule 41 violation, regardless of good intentions or
02:19:35PM 18 investigatory need, or anything like that. It is required
02:19:39PM 19 if the violation was deliberate. We believe it clearly
02:19:45PM 20 was deliberate. DOJ's own policies and internal analysis
02:19:49PM 21 of Rule 41 that we cited at length to the court actually
02:19:52PM 22 tracks Weiland and the Rule 41 analysis.

02:19:57PM 23 Now, I can appreciate that internet crime is hard to
02:20:00PM 24 investigate. And I do not think that any of the gentlemen
02:20:05PM 25 sitting here are malicious in the sense that it has been

02:20:10PM 1 used in this courtroom. But what I do believe is that
02:20:13PM 2 this was deliberate.

02:20:15PM 3 And regardless of whether it was deliberate, we know
02:20:17PM 4 that this is an issue of constitutional magnitude, which
02:20:21PM 5 is the other Weiland factor. Because as your Honor just
02:20:24PM 6 heard, we are dealing with core privacy issues and the
02:20:27PM 7 ability of the courts to oversee the application of
02:20:32PM 8 executive powers.

02:20:37PM 9 And unless and until the Supreme Court changes
02:20:40PM 10 Rule 41, those are the rules. Those are the rules. And
02:20:44PM 11 there is no question the Department of Justice knows that.

02:20:47PM 12 THE COURT: What do you make of Rule 3103a? That
02:20:55PM 13 seems to open a door, but there is not, to my knowledge,
02:21:01PM 14 much law about how it applies.

02:21:03PM 15 MR. FIEMAN: Your Honor, I think we responded to
02:21:07PM 16 what 3103a was directed to, which is --

02:21:10PM 17 THE COURT: Pardon me?

02:21:11PM 18 MR. FIEMAN: I'm sorry. You are talking about
02:21:12PM 19 3103a?

02:21:14PM 20 THE COURT: Yeah.

02:21:16PM 21 MR. FIEMAN: Correct. But that is addressing the
02:21:18PM 22 mere evidence rule. We are not disputing that they had --
02:21:20PM 23 they could legally seize evidence, data, if they had a
02:21:25PM 24 proper warrant to do it.

02:21:32PM 25 Now, your Honor, I think where this is ultimately

going to end up -- And that Rule 41 issue, your Honor, is entirely different from what the face of the warrant says. That is a core Fourth Amendment principle, but the scope of the search or the location of the search cannot exceed the jurisdictional boundaries that appear on the face of the warrant. That is just hornbook Ninth Circuit law.

THE COURT: Part of the question is, if there was a violation of Rule 41, what should be done about it. And I know your position is that it demands suppression. I asked the question, what if a district judge had issued this warrant instead of the magistrate judge, what difference would it have made?

MR. FIEMAN: Ultimately no difference, your Honor, because if the district court had signed a warrant that says that the location of the search is the Eastern District of Pennsylvania, period, that is it. That decision by the judge, whether it is magistrate judge or district court judge, that is the scope of the authorization, that is the limits of the geographic boundaries of the search. And that is separate and apart from Rule 41.

THE COURT: So you are saying that there is no way to get a warrant that would address the particular problem or issue that the government faced in this case?

MR. FIEMAN: First of all -- Two things, your

02:23:18PM 1 Honor: That problem needs to be directed to the Supreme
02:23:25PM 2 Court and the rules committee in Congress, if and when
02:23:27PM 3 they decide that weighing the privacy interests --

02:23:30PM 4 THE COURT: So they find an answer in five or ten
02:23:33PM 5 years. Those guys don't move very fast.

02:23:36PM 6 MR. FIEMAN: Meanwhile, the government needs to
02:23:39PM 7 respect the law as it stands.

02:23:40PM 8 More importantly, there are alternatives. We have
02:23:44PM 9 seen plenty of, in this court alone, child pornography
02:23:50PM 10 investigations, where, for example, you have targets
02:23:56PM 11 visiting illicit websites, the undercover has engaged in
02:24:01PM 12 messages, they exchange emails, they redirect them to
02:24:06PM 13 sites in the jurisdiction where they want to get a
02:24:09PM 14 warrant. What they could have done, for example, is --
02:24:12PM 15 We talked a little bit about spoofing. You can redirect
02:24:15PM 16 someone from the homepage when they go into the site into
02:24:19PM 17 servers located anywhere that you want them to go. It
02:24:22PM 18 takes more effort, that's true. Sometimes doing things
02:24:26PM 19 right and legally does take more effort. But they were
02:24:30PM 20 not without investigatory alternatives.

02:24:33PM 21 And here, ultimately, your Honor, even if they were,
02:24:37PM 22 which just simply is not the case, the investigatory ends
02:24:43PM 23 cannot justify illegal means. And I mean "illegal" in the
02:24:48PM 24 sense that they didn't follow what was on the face of the
02:24:51PM 25 warrant, they didn't follow Rule 41, I believe they were

02:24:55PM 1 not candid with Judge Buchanan, and all the things that we
02:24:59PM 2 have probably briefed to death, your Honor.

02:25:02PM 3 Now, in some ways this seems like a somewhat
02:25:09PM 4 old-fashioned, simple way to resolve a complicated case,
02:25:13PM 5 because we know you have to go by what the warrant says.

02:25:21PM 6 Hopefully if the court rules against the government --
02:25:23PM 7 Please bear in mind this is a situation of their own
02:25:26PM 8 making. Why didn't they get a warrant from Judge Buchanan
02:25:31PM 9 that said United States of America -- person or property
02:25:34PM 10 located in the United States of America, persons and
02:25:36PM 11 property -- like they did in the other case before Judge
02:25:40PM 12 Smith's decision, and they knew they had a problem, that
02:25:42PM 13 say Eastern District of Virginia and elsewhere? That is
02:25:47PM 14 something they should have tried for, that they could have
02:25:51PM 15 tried for. And if Judge Buchanan thought that was legal
02:25:55PM 16 and appropriate, we would probably be arguing a separate
02:25:58PM 17 set of issues. They didn't do that. And I think we have
02:26:02PM 18 laid out why.

02:26:04PM 19 Their investigatory ends may have been justifiable,
02:26:10PM 20 but their means were unconstitutional. Thank you, your
02:26:15PM 21 Honor.

02:26:21PM 22 THE COURT: Mr. Becker. Let's take ten so I don't
02:26:25PM 23 interrupt you.

02:38:50PM 24 (Break.)

02:38:50PM 25 THE COURT: Mr. Becker.

02:38:52PM 1 MR. BECKER: Thank you, your Honor. Appreciate
02:38:54PM 2 the recess. Your Honor, I will start with the broader
02:39:01PM 3 picture from our perspective, which is that in this
02:39:06PM 4 investigation law enforcement identified and recognized a
02:39:11PM 5 serious problem of illegal activity occurring in a way
02:39:17PM 6 that was technically advanced that required action. And
02:39:26PM 7 in the course of pursuing that investigation, and
02:39:30PM 8 obtaining process in order to obtain evidence, went to the
02:39:35PM 9 courts and sought authorization to use lawful techniques
02:39:40PM 10 and court-authorized techniques to counter the sort of
02:39:43PM 11 challenge they faced from criminals committing crimes and
02:39:47PM 12 exploiting children using an advanced technology. That is
02:39:51PM 13 the problem that law enforcement faced in this case. And
02:39:54PM 14 I think that is the light in which the court should view
02:39:57PM 15 the various issues in this case, because that's what is at
02:40:01PM 16 issue.

02:40:01PM 17 This is a criminal case. It is a child pornography
02:40:03PM 18 case. It pertains to a website on which users were
02:40:08PM 19 engaging in the trafficking of child pornography. And
02:40:10PM 20 that is what it is about, it is about criminal
02:40:14PM 21 enforcement, and the tools that law enforcement uses in
02:40:18PM 22 order to counter the tools that criminals use. That is
02:40:20PM 23 the context we are in.

02:40:22PM 24 I will start with the Rule 41 issue. Undoubtedly --
02:40:26PM 25 You know, we disagree in terms of the defense's read of

02:40:30PM 1 Rule 41. We have set that forth in our papers. I won't
02:40:34PM 2 belabor that issue.

02:40:35PM 3 The Supreme Court has said very clearly that Rule 41
02:40:39PM 4 is to be interpreted flexibly. We do believe that it can
02:40:42PM 5 be interpreted to allow the sort of search that the
02:40:45PM 6 magistrate authorized in this case.

02:40:49PM 7 But we think it makes more sense for the court to
02:40:52PM 8 focus on the question of whether or not -- And we don't
02:40:55PM 9 believe it is necessary for the court to decide that
02:40:57PM 10 particular issue, because we do believe it is absolutely
02:41:00PM 11 clear that suppression for a violation or purported
02:41:04PM 12 violation of Rule 41 in this case is not warranted for a
02:41:10PM 13 number of reasons.

02:41:11PM 14 So suppression, according to the Ninth Circuit, would
02:41:15PM 15 be warranted generally only for a fundamental violation,
02:41:18PM 16 that is, a violation of constitutional magnitude. And
02:41:22PM 17 that is not what happened in this case, because the
02:41:25PM 18 pillars of the Fourth Amendment were complied with by law
02:41:32PM 19 enforcement.

02:41:32PM 20 The FBI requested and obtained a warrant from a
02:41:35PM 21 neutral and detached magistrate based on a finding of
02:41:38PM 22 probable cause, certainly from our perspective a strong
02:41:41PM 23 showing of probable cause, that obviously the magistrate
02:41:44PM 24 judge agreed with in authorizing the warrant.

02:41:47PM 25 The other pillars of the Fourth Amendment were

02:41:50PM 1 complied with, that is, probable cause particularly
02:41:56PM 2 describing the information to be seized. The
02:42:00PM 3 particularity requirement is met here. It is absolutely
02:42:04PM 4 clear from the warrant exactly what information law
02:42:06PM 5 enforcement may collect and did collect pursuant to the
02:42:09PM 6 warrant itself.

02:42:09PM 7 We think it is clear there is no basis for suppression
02:42:12PM 8 based on an argument there was a fundamental or
02:42:15PM 9 constitutional violation in this context, where law
02:42:18PM 10 enforcement goes to a court for authorization to do
02:42:20PM 11 exactly what it is asking for authorization to do, that
02:42:23PM 12 authorization is granted, the warrant describes -- meets
02:42:26PM 13 the particularity requirement. That is obviously very
02:42:29PM 14 clear and really spelled out exactly what this warrant is
02:42:32PM 15 designed to collect.

02:42:34PM 16 Without that being a fundamental violation, a mere
02:42:42PM 17 technical violation of Rule 41 would properly result in
02:42:45PM 18 suppression only where the defendant can establish
02:42:48PM 19 prejudice or intentional and deliberate disregard, a
02:42:51PM 20 violation of the rule.

02:42:52PM 21 I will start with the intentional or deliberate
02:42:55PM 22 violation. There is simply no evidence of that in this
02:42:58PM 23 case. There is no controlling law that was out there that
02:43:01PM 24 said that a magistrate authorizing this sort of search
02:43:06PM 25 would be or is a violation of Rule 41. There is one

02:43:10PM 1 magistrate's opinion that exists, from a magistrate who --
02:43:17PM 2 law enforcement applied for that warrant, and the
02:43:18PM 3 magistrate rejected it. That could happen in any
02:43:21PM 4 scenario. That could happen every time law enforcement
02:43:24PM 5 applies for a search warrant.

02:43:25PM 6 That doesn't indicate -- Certainly if and when law
02:43:29PM 7 enforcement goes, in a different scenario, regarding a
02:43:32PM 8 different investigative technique, to a different
02:43:34PM 9 magistrate in a different investigation, and requests
02:43:36PM 10 authority for that particular investigative technique,
02:43:39PM 11 that just because some magistrate elsewhere in a different
02:43:43PM 12 case had rejected a warrant, that by requesting that
02:43:46PM 13 authority for something different, if arguably similar,
02:43:49PM 14 makes it an intentional or deliberate violation of the
02:43:52PM 15 rule, particularly in light of the fact, as this court is
02:43:56PM 16 aware, and is clearly noted in this record, other
02:43:58PM 17 magistrate judges have approved network investigative
02:44:01PM 18 techniques in similar scenarios to this one.

02:44:04PM 19 And so among that landscape, where you have a
02:44:07PM 20 magistrate who has rejected a warrant, arguably similar, a
02:44:11PM 21 number of magistrates who have approved warrants arguably
02:44:15PM 22 similar, I think it is impossible to say that law
02:44:17PM 23 enforcement is acting with a deliberate disregard of the
02:44:19PM 24 rule by presenting the facts in the investigation to a
02:44:22PM 25 neutral and detached magistrate who decides there is

02:44:24PM 1 probable cause and this warrant should issue.

02:44:28PM 2 The other side of the technical violation would be
02:44:33PM 3 prejudice, and that is the prejudice in that if the rule
02:44:37PM 4 had been followed, the search would not have occurred.

02:44:42PM 5 And here, the defendant's argument falls flat, because
02:44:46PM 6 his prejudice argument is that no court ever, anywhere,
02:44:49PM 7 could ever authorize a search of Mr. Michaud's computer,
02:44:53PM 8 or any of the users of this particular website, purely
02:44:57PM 9 because they decided to use the Tor network, and therefore
02:44:59PM 10 that makes them immune to any court-authorizing process in
02:45:03PM 11 order to take steps to identify their location; that
02:45:07PM 12 because their location is unknown at the time, no court
02:45:12PM 13 may authorize investigative steps in order to identify
02:45:15PM 14 them. That is not the sort of prejudice this court should
02:45:19PM 15 account, not the sort of prejudice that is called for and
02:45:21PM 16 certainly focused on in the law talking about prejudice in
02:45:26PM 17 terms of a technical error.

02:45:28PM 18 There are cases where at a time where the location of
02:45:32PM 19 the search is known, so either the object of the search
02:45:36PM 20 was a house in a known location, a car in a known
02:45:40PM 21 location, that was outside of the magistrate's district,
02:45:42PM 22 that prejudice has been found. But that's not this case.
02:45:45PM 23 In this case the location of the user is unknown, and the
02:45:50PM 24 technique is being applied for and requested precisely in
02:45:53PM 25 order to find information that will help locate that user,

02:45:58PM 1 the information about it. So a very, very different
02:46:00PM 2 context here.

02:46:01PM 3 And so, ultimately, your Honor, we think the
02:46:05PM 4 suppression argument fails, because law enforcement acted
02:46:08PM 5 reasonably in account of all of the circumstances of the
02:46:12PM 6 investigation, by going to a magistrate, articulating
02:46:18PM 7 probable cause, and articulating what would happen to the
02:46:22PM 8 warrant and whose computers would be searched.

02:46:24PM 9 We don't agree certainly with the defense's argument
02:46:27PM 10 that somehow the magistrate was misled, or did not or
02:46:30PM 11 would not have understood that the request was to search
02:46:34PM 12 computers that accessed this website wherever they were
02:46:37PM 13 located. That is because the warrant affidavit
02:46:39PM 14 specifically says, on Page 29, "It is respectfully
02:46:46PM 15 requested that the court issue a search warrant
02:46:49PM 16 authorizing the following: The NIT may cause an active
02:46:53PM 17 computer, wherever located, to send to a computer
02:46:55PM 18 controlled to or known by the government," and then it
02:46:58PM 19 goes through the sort of information that it is requesting
02:47:02PM 20 to be delivered.

02:47:02PM 21 In light of that, as well as the warrant application
02:47:05PM 22 as a whole, makes it unmistakably clear that the purpose
02:47:09PM 23 of the warrant and the technique is to identify the
02:47:12PM 24 locations of users' computers who are then -- whose
02:47:16PM 25 location is at that time unknown.

02:47:19PM 1 So I don't think there is any fair read of this
02:47:21PM 2 application that could show the magistrate was misled
02:47:26PM 3 about the purpose of the warrant, or the fact that it was
02:47:29PM 4 requesting authority to be deployed to computers, wherever
02:47:35PM 5 they were located. It is right there in the application.

02:47:37PM 6 Now, in terms of the warrant itself, the defendant
02:47:40PM 7 just sort of -- in his argument that it was cabined into
02:47:46PM 8 computers only in the Eastern District of Virginia, the
02:47:49PM 9 defendant really reads out the warrant attachment.

02:47:53PM 10 And that is, Attachment A of the warrant, incorporated
02:47:57PM 11 into the warrant, makes it clear that the activating
02:47:59PM 12 computers are those of any user or administrator who logs
02:48:03PM 13 into the target website by entering a user name and
02:48:06PM 14 password. It does not say any user or administrator
02:48:11PM 15 located only in the Eastern District of Virginia. The
02:48:14PM 16 warrant clearly requested authority to deploy to computers
02:48:17PM 17 wherever located.

02:48:18PM 18 And I don't believe, again, it is a fair read of the
02:48:20PM 19 attachment to say -- particularly where it specifies that
02:48:24PM 20 the server is located in the Eastern District of Virginia,
02:48:28PM 21 and then authorizes on activated computers of any user or
02:48:35PM 22 administrator who logs into the target site, that that is
02:48:40PM 23 somehow cabined in, or that that was the intent of the
02:48:41PM 24 magistrate in authorizing it.

02:48:43PM 25 The application makes unmistakably clear what sort of

02:48:45PM 1 authority the government was requesting. And that is the
02:48:47PM 2 authority that the magistrate -- certainly we would argue
02:48:50PM 3 that the magistrate was granting in approving of this
02:48:54PM 4 warrant, as she did.

02:48:58PM 5 In terms of -- Your Honor had a question about the
02:49:05PM 6 location of the search. Here, we are dealing in a
02:49:09PM 7 context, which we think is clear, where there are two-way
02:49:13PM 8 communications going on between users and a computer
02:49:16PM 9 server.

02:49:17PM 10 But there is no question that at the time the NIT is
02:49:20PM 11 authorized, at the time the NIT is deployed, the computer
02:49:22PM 12 server onto which that NIT code is deployed is in the
02:49:26PM 13 Eastern District of Virginia. The computers of -- the
02:49:29PM 14 activating computers, the users, are communicating with
02:49:32PM 15 the Eastern District of Virginia when they access that
02:49:36PM 16 website, that two-way communication that is going on. The
02:49:39PM 17 information that is collected by the NIT is returned to a
02:49:42PM 18 computer in the Eastern District of Virginia.

02:49:45PM 19 And so in requesting this authority, and with the
02:49:49PM 20 warrant being authorized, law enforcement is going to the
02:49:52PM 21 district that has the closest, strongest connection to all
02:49:55PM 22 of the communications that are pertinent. The warrant
02:49:59PM 23 deals with users who are making a voluntary choice to step
02:50:02PM 24 into the Eastern District of Virginia and access that
02:50:05PM 25 website. And that's where they get that code.

02:50:08PM 1 It is certainly true that the code then goes to that
02:50:11PM 2 user's computer, as described in the warrant, and then
02:50:15PM 3 returns -- has to go to that user's computer, wherever
02:50:18PM 4 located, in this situation it was here in Washington, and
02:50:22PM 5 then return the information back to the Eastern District
02:50:24PM 6 of Virginia.

02:50:26PM 7 I don't think it is a fair analysis, though, to say
02:50:29PM 8 that means the search occurred only in Washington, because
02:50:33PM 9 that -- it reads out -- that sort of analysis would have
02:50:36PM 10 to read out this two-way factor sort of communication that
02:50:41PM 11 is going on, and the fact that the user is entering the
02:50:45PM 12 Eastern District of Virginia when the communications are
02:50:47PM 13 taking place.

02:50:49PM 14 The other aspect, your Honor, that we would ask you to
02:50:52PM 15 consider is certainly the good-faith argument here. And
02:50:55PM 16 that is that law enforcement in this case acted in
02:50:58PM 17 objectively reasonable reliance upon the authorization of
02:51:02PM 18 a magistrate, who found probable cause, who found
02:51:07PM 19 particularity, who authorized the particular technique
02:51:10PM 20 that law enforcement applied for.

02:51:12PM 21 This is not a scenario where law enforcement was
02:51:15PM 22 granted a warrant and then took some action in the
02:51:18PM 23 execution that was somehow different than what they
02:51:21PM 24 applied for, or outside of what they applied for, which
02:51:24PM 25 might justify suppression, such as a case where law

02:51:29PM 1 enforcement, which is -- when they are required to leave a
02:51:31PM 2 copy of a warrant in a premises, deliberately decides not
02:51:34PM 3 to do so, and not with any authority from the court.

02:51:38PM 4 Here, law enforcement acted expressly within their
02:51:44PM 5 articulated requests to the magistrate, and that is the
02:51:46PM 6 website operates in the Eastern District of Virginia, the
02:51:49PM 7 NIT gets deployed to the activated computers wherever
02:51:54PM 8 located, and returns information to the Eastern District
02:51:55PM 9 of Virginia. Law enforcement relied in good faith on that
02:51:59PM 10 authorization. And so that's a further reason, your
02:52:03PM 11 Honor, why suppression is inappropriate in this scenario.

02:52:08PM 12 The one other issue that we would present to the
02:52:15PM 13 court, if I may tender it, just today -- And I referenced
02:52:18PM 14 this earlier. May I approach?

02:52:20PM 15 THE COURT: Yes. I think somebody put a copy of
02:52:28PM 16 this on my desk. I already have a copy of it.

02:52:36PM 17 MR. BECKER: Just today, your Honor, a report and
02:52:38PM 18 recommendation was filed in the case of United States
02:52:39PM 19 versus Epic. It is 15 -- for the record, 15CR163, Docket
02:52:49PM 20 No. 53. In that case the same network investigative
02:52:54PM 21 technique warrant, as in this case, was challenged on a
02:52:57PM 22 motion to suppress. That defendant raised a Rule 41
02:53:01PM 23 challenge, as well as a probable cause challenge to the
02:53:04PM 24 warrant. That magistrate has reported to the district
02:53:07PM 25 judge, finding sufficient probable cause to support the

02:53:11PM 1 issuance of the warrant, declining to ultimately rule on
02:53:14PM 2 the Rule 41 issue, but finding, nonetheless, suppression
02:53:17PM 3 was inappropriate in this scenario. And so that is what
02:53:22PM 4 we would propose your Honor rule.

02:53:24PM 5 We think, again, we have made our Rule 41 argument,
02:53:28PM 6 but that ultimately it is not necessary, that law
02:53:32PM 7 enforcement acted reasonably here, and that suppression is
02:53:35PM 8 not warranted. So we would request that your Honor deny
02:53:37PM 9 the defendant's motions to suppress. Thank you.

02:53:40PM 10 THE COURT: Let me ask you a couple of questions.
02:53:42PM 11 One of the things I commented on was, what does 3103a mean
02:53:53PM 12 in light of this role argument?

02:53:56PM 13 MR. BECKER: We have reviewed it, your Honor. We
02:53:58PM 14 don't believe, and wouldn't make the argument, that that
02:54:01PM 15 would provide sort of an independent basis from Rule 41 in
02:54:07PM 16 order for a district court or a magistrate judge to
02:54:10PM 17 authorize the warrant. I think, having briefly researched
02:54:14PM 18 it, it was a more sort of discrete purpose. I don't think
02:54:19PM 19 the defense is necessarily -- I think the defense may be
02:54:21PM 20 correct in terms of the purpose of the amendment to that
02:54:23PM 21 statute. And so we are not arguing that that would impact
02:54:27PM 22 the court's analysis here.

02:54:30PM 23 THE COURT: What difference would it make if a
02:54:35PM 24 district judge had issued this warrant?

02:54:38PM 25 MR. BECKER: While we think it is something the

02:54:40PM 1 court can consider, in terms of the reasonableness of law
02:54:43PM 2 enforcement's actions, that a district judge did approve a
02:54:46PM 3 wiretap in this case, which allowed for the collection of
02:54:50PM 4 a much greater set of evidence, that is, the ongoing
02:54:54PM 5 collection of content, which a district judge found
02:54:57PM 6 appropriate, and that the court consider that in terms of
02:55:01PM 7 the overall reasonableness of the government's conduct, we
02:55:03PM 8 don't think it would make a difference -- we wouldn't
02:55:06PM 9 argue it makes a difference in terms of a Rule 41 analysis
02:55:09PM 10 if a district judge had authorized the search.

02:55:17PM 11 THE COURT: Let me ask you one other question. If
02:55:34PM 12 a good warrant is issued for material in the state of
02:55:49PM 13 Washington, and the search turns up information of a crime
02:55:54PM 14 in an adjoining state -- That's not what you went after
02:56:03PM 15 to begin with, but very often drug dealers keep records,
02:56:08PM 16 and so forth. So you have information then about a crime
02:56:14PM 17 in another state. You are free to use that information
02:56:18PM 18 going after a criminal in the adjoining state, are you
02:56:22PM 19 not?

02:56:22PM 20 MR. BECKER: We believe that to be true, your
02:56:26PM 21 Honor. It is sort of a plain-view type argument that we
02:56:32PM 22 do think could be justified here. And so if under the
02:56:36PM 23 defense view only searches of computers in EDVA were
02:56:42PM 24 authorized, but during the course of that authorized
02:56:45PM 25 conduct that they would, I gather, concede it was

02:56:48PM 1 appropriate, at least for EDVA computers, information
02:56:52PM 2 pertaining to criminal acts and criminal evidence of other
02:56:56PM 3 computers was observed by law enforcement in plain view, I
02:57:01PM 4 do think that would be -- could be a reason that law
02:57:05PM 5 enforcement would be able to use that evidence in a
02:57:07PM 6 criminal prosecution, and it would not necessarily be
02:57:10PM 7 suppressible. I have a brief note on that. I will leave
02:57:36PM 8 that there, your Honor.

02:57:37PM 9 The last point I would make -- the one thing we
02:57:40PM 10 haven't discussed in terms of the reasonableness, and kind
02:57:43PM 11 of bringing this back to the evidence, is that the IP
02:57:48PM 12 address information is really different in quality than
02:57:51PM 13 the MAC address information, in that IP address
02:57:55PM 14 information, this circuit, other circuits, have
02:57:58PM 15 consistently found not to be something over which a user
02:58:02PM 16 has a reasonable expectation of privacy. It is the IP
02:58:05PM 17 address information that ultimately furnishes the probable
02:58:09PM 18 cause in order to ultimately have a residential search
02:58:11PM 19 warrant granted, and for the evidence that ultimately was
02:58:15PM 20 found on Mr. Michaud's devices to be seized.

02:58:19PM 21 So here, when we are talking about the fundamental
02:58:24PM 22 violation issue, the reasonableness issue, we do think the
02:58:27PM 23 court is right to consider the limited scope of the search
02:58:30PM 24 that was authorized and conducted in this case.

02:58:33PM 25 This wasn't a full-blown search of everything in

02:58:36PM 1 someone's home, or even everything on someone's computer.
02:58:40PM 2 This is a search that delivered information that was
02:58:43PM 3 limited, that was targeted, and with respect to the IP
02:58:46PM 4 address information, that users do not have a reasonable
02:58:49PM 5 expectation of privacy over. And even while communicating
02:58:53PM 6 over Tor, that doesn't change the nature of the
02:58:56PM 7 communication, or that IP address information, which
02:59:00PM 8 belongs to an internet service provider, not to any
02:59:02PM 9 individual.

02:59:04PM 10 And so we do think that is a factor, as the court
02:59:09PM 11 hones in on what is really the piece of evidence that
02:59:12PM 12 matters in terms of going forward, it is that IP address
02:59:15PM 13 information. Again, a limited, focused search that was
02:59:18PM 14 conducted here contributed to its reasonableness.

02:59:26PM 15 If the court has no further questions, thank you, your
02:59:28PM 16 Honor.

02:59:29PM 17 THE COURT: Thank you, Mr. Becker.

02:59:37PM 18 MR. FIEMAN: Your Honor, since I have the burden,
19 can I have a couple of minutes to respond?

02:59:38PM 20 Let me knock out a couple of simple points that
02:59:41PM 21 Mr. Becker said, and then get back to the crux of this.
02:59:44PM 22 The privacy interest is not the IP address. The privacy
02:59:48PM 23 interest is Mr. Michaud's home. It is like saying you
02:59:51PM 24 have a telephone number, and the government can't tell
02:59:56PM 25 where you are calling from because you have caller ID

02:59:59PM 1 blocking, well, then it is just fine to go into somebody's
03:00:03PM 2 house and take their address book.

03:00:05PM 3 We have cited several times that the quality or
03:00:08PM 4 quantity of information or evidence seized is irrelevant
03:00:10PM 5 for Fourth Amendment purposes. And if there was no
03:00:14PM 6 privacy interest, and this was shared with the service
03:00:17PM 7 provider, they could have gone to Comcast and asked for
03:00:20PM 8 it. But they couldn't and they didn't.

03:00:23PM 9 The question then is whether this intrusion on
03:00:26PM 10 Mr. Michaud's home, whether it is for a matchbook or kilos
03:00:30PM 11 of drugs, doesn't matter. It is the intrusion, not the
03:00:33PM 12 information that is taken, that is protected by the Fourth
03:00:36PM 13 Amendment. So that, we firmly believe, is a red herring.

03:00:40PM 14 Your Honor, I think Mr. Becker interpreted this
03:00:43PM 15 question as helpful to the government in terms of if, for
03:00:47PM 16 example, in the course of operating the Virginia website
03:00:50PM 17 there was information in plain view or had been turned up
03:00:55PM 18 in the course of operating that site, that would have led
03:00:58PM 19 them to believe they could conduct a search in another
03:01:01PM 20 jurisdiction.

03:01:02PM 21 Well, two things would have happened. Let me point
03:01:05PM 22 out two things. One is, they did not get the information
03:01:08PM 23 and data from the Virginia server. They have not
03:01:11PM 24 contested at this point that the data extraction, the
03:01:16PM 25 search, occurred in Washington. That is true.

03:01:17PM 1 If they had gone back through their server records and
03:01:19PM 2 found an IP address associated with Pewter, or anybody, in
03:01:23PM 3 the course of exercising that Virginia warrant, and then
03:01:27PM 4 took that information, went to Comcast, said we now know
03:01:31PM 5 this is a Washington address, and then came to this court
03:01:34PM 6 and asked for a warrant, that is the way it is supposed to
03:01:36PM 7 work.

03:01:38PM 8 So this is not a plain-view situation, because they
03:01:41PM 9 never saw it in Virginia. They had to search
03:01:44PM 10 Mr. Michaud's home to find it. It is a little like saying
03:01:46PM 11 if I drive my car into Virginia, you can search my
03:01:49PM 12 Washington home, if that is the only connection.

03:01:51PM 13 Your Honor, let me also say that the Title III
03:01:55PM 14 authorization specifically said that the NIT warrant
03:02:00PM 15 application was going to be separate. This isn't a
03:02:03PM 16 Title III case, because it doesn't deal with those
03:02:05PM 17 communications.

03:02:06PM 18 The Epic decision only addressed probable cause, did
03:02:11PM 19 not reach the issues that we briefed here.

03:02:14PM 20 Let me talk briefly about the probable cause issue.
03:02:18PM 21 We have, according to the government, a warrant that
03:02:20PM 22 authorizes up to 100,000 searches, because that is the
03:02:24PM 23 number of account users that accessed while the FBI was
03:02:27PM 24 operating this site.

03:02:29PM 25 It is a site, your Honor, that does not, even

03:02:31PM 1 according to the criteria that we have seen from Gourde
03:02:35PM 2 and the other cases, unabashedly announce it is illegal.

03:02:39PM 3 I will put this back up. The court has seen it many
03:02:40PM 4 times. What we are talking about is -- Is that the
03:02:45PM 5 correct way for it to face for your Honor? We are talking
03:02:48PM 6 about something that has a teenager who is -- I have seen
03:02:54PM 7 in my daughter's Sixteen magazine much more skin or
03:02:59PM 8 provocation. It advertises itself as a chat room. There
03:03:02PM 9 is no reference to child pornography. There is no
03:03:07PM 10 indication that this is anything more than a fetish site
03:03:12PM 11 or chat room. It doesn't even have what arguably would
03:03:15PM 12 qualify as lascivious pornography on it.

03:03:20PM 13 As your Honor has recognized in other cases, the scope
03:03:22PM 14 of the search has to be firmly grounded in the probable
03:03:26PM 15 cause -- the extent to which probable cause is
03:03:31PM 16 established.

03:03:32PM 17 Now, this would be a close call if we were dealing
03:03:35PM 18 with one search. I argued the Gourde case, and the Martin
03:03:39PM 19 cases. And that's why the court created something of a
03:03:44PM 20 bright line, because of the inability often to segregate
03:03:50PM 21 legal, if maybe distasteful, activities that are protected
03:03:54PM 22 from things that clearly establish an illicit illegal
03:03:59PM 23 intent.

03:04:00PM 24 This warrant authorized the deployment of 100,000
03:04:03PM 25 searches anywhere in the world based upon what is on that

03:04:06PM 1 web page. That is a pretty slim read on which to hang
03:04:11PM 2 such an unprecedented sweeping authorization.

03:04:17PM 3 Now, your Honor, in terms of that authorization, you
03:04:20PM 4 can look at the attachments, and there is not one word,
03:04:24PM 5 not one word, about this warrant being executed outside
03:04:28PM 6 the Eastern District of Virginia. And just compare what
03:04:33PM 7 the government did in 2012, where they submitted a warrant
03:04:38PM 8 that indicates that the searches -- the deployment of a
03:04:42PM 9 NIT in this Texas slayer case -- actually, the defendant
03:04:46PM 10 has not been apprehended, but they got a warrant, clearly
03:04:49PM 11 states that the NIT will be deployed in Colorado and
03:04:52PM 12 elsewhere. Now, if that particular defendant is ever
03:04:57PM 13 apprehended, there may be good Rule 41 issues. But we are
03:05:00PM 14 not at the Rule 41 issues.

03:05:02PM 15 What they have here, by their own submission, is a
03:05:07PM 16 warrant that says Eastern District of Virginia, period.
03:05:13PM 17 They drafted that. That's what they presented to Judge
03:05:20PM 18 Buchanan.

03:05:22PM 19 And even if they are now hung on the horns of their
03:05:25PM 20 own dilemma, your Honor, the law is clear, the search
03:05:30PM 21 warrant controls. And if the search occurs outside the
03:05:35PM 22 authorized scope of the warrant or location authorized,
03:05:40PM 23 then suppression is mandated. Good faith is irrelevant.

03:05:43PM 24 So if I get a warrant that says I am going to search
03:05:48PM 25 2304 Elm Drive, and I decide I am going to search 1606

Apple Lane, and 1405 President Street, it doesn't matter what you intended, it is an illegal search.

It only bears repeating, your Honor, that this is the warrant they drafted, and there is nothing in the attachment that changes it.

And they have some choices. They have some options. They can resubmit the warrants in future investigations that candidly say that they are United States in scope. They can pursue the rule changes, which would be decided by the end of this year.

Even if Rule 41 changes, they still need to put on the face of the warrant, regardless of the rule, the locations where they are searching.

Your Honor, to come back to this, we are dealing in some ways with new territory. But the Fourth Amendment principles and guidelines are well established. It is exactly the kind of governmental overreaching, or the ability to conduct seemingly endless searches on the basis of a single authorization, that drove a lot of what the founders were concerned about with general warrants. It does require care, candor, and specificity in order to get a valid warrant that is as sweeping as this one.

Your Honor, however this ultimately rules out -- maybe it is a matter of this case going up alongside *Essick*, and it may ultimately be a decision for the Supreme Court, but

03:07:33PM 1 unless we are going to not only -- just forget about 41,
03:07:36PM 2 ignore what is on the face of the warrant, and disregard
03:07:39PM 3 the constitutional guidelines that really are the core
03:07:42PM 4 issue in this case, suppression is not only the
03:07:47PM 5 appropriate and necessary remedy, it is something that is
03:07:51PM 6 desperately needed, so that these issues can be resolved
03:07:55PM 7 in a way that protects core privacy interests in the face
03:07:59PM 8 of such sweeping governmental authority.

03:08:05PM 9 I respectfully disagree with Mr. Becker about the
03:08:08PM 10 investigatory alternatives that are available. I
03:08:10PM 11 respectfully disagree with him about their intentions in
03:08:14PM 12 presenting this warrant to Judge Buchanan. I do respect
03:08:19PM 13 that he is a law enforcement officer with good intentions
03:08:23PM 14 personally, all of which is irrelevant. The warrant says
03:08:28PM 15 what it says.

03:08:29PM 16 And when we have all of this background, and the scale
03:08:32PM 17 of such an unprecedented search, and such paucity of PC to
03:08:37PM 18 begin with on the face of this homepage, your Honor, it
03:08:41PM 19 seems to me that suppression is not only appropriate but
03:08:45PM 20 required in every view of the law that we have presented
03:08:49PM 21 to the court. Thank you.

03:08:50PM 22 THE COURT: Thank you. Well, you know, I have
03:08:56PM 23 been at this a long time, 45-plus years. I have issued, I
03:09:07PM 24 don't know, probably hundreds of search warrants. I have
03:09:11PM 25 ruled on suppression motions hundreds of times, I suppose,

03:09:15PM 1 over that period. This is likely the most complex one
03:09:19PM 2 yet. The hearing today has clarified a number of things
03:09:27PM 3 that were in my mind. But I've got to read your prolix
03:09:36PM 4 brief again, the warrant applications, and the warrants
03:09:40PM 5 and put this together.

03:09:46PM 6 I've got no hearings or trials for the next week, so
03:09:51PM 7 this is on top of the pile, and I should be able to get
03:09:54PM 8 you an answer by the middle of the week next week, either
03:10:02PM 9 in writing or, if I choose to do it orally, if you are not
03:10:05PM 10 in town we can do it on the telephone. I typically rule
03:10:09PM 11 orally when I can. I am not ready to rule yet. I will
03:10:18PM 12 let you know as soon as I can, and we will get you an
03:10:22PM 13 answer. Thank you.

14 (Proceedings adjourned.)
15
16
17
18
19
20
21
22
23
24
25

